UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

NAICOM CORPORATION, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	No. 3:21-cv-01405-JAW
	)	
DISH NETWORK CORPORATION, et al.,	)	
	)	
Defendants.	)	

ORDER ON FEDERAL DEFENDANTS' MOTION TO DISMISS

A set of federal-employee defendants moves to dismiss plaintiffs' seven-count complaint, arising from federal agents searching plaintiffs' business and seizing their intellectual property. The Court grants the motion to dismiss, dismissing all seven counts. At the outset, based on the allegations in the complaint, the Court determines that the prosecutor defendants are entitled to absolute prosecutorial immunity on all counts. The Court dismisses the RICO claims (Counts I & II) because plaintiffs have not adequately pleaded an enterprise, a pattern of racketeering activity, or a conspiracy. The Court dismisses the Computer Fraud and Abuse Act claim (Count III), the Stored Communications Act claim (Count IV), the Digital Millennium Copyright Act claim (Count V), and the Defend Trade Secrets Act claim (Count VI) because the alleged conduct falls within statutory exceptions for authorized law enforcement activity. Finally, the Court dismisses the Puerto Rico Uniform Trade Secrets Act claim because the defendants must be substituted pursuant to the

Westfall Act and plaintiffs have not complied with the procedural requirements of the Federal Tort Claims Act.

I. PROCEDURAL HISTORY

On August 27, 2021, Naicom Corporation, D&V IP Holdings, LLC, Paylink, LLC, and Kiaras, LLC, filed a seven-count complaint against approximately twenty known Defendants and two dozen unknown Defendants.[1] *Compl.* (ECF No. 1). The Court has twice permitted Plaintiffs to amend their complaint, and the Second Amended Complaint is now the operative complaint. *Am. Compl.* (ECF No. 100); *Second Am. Compl.* (ECF No. 130).

The parties categorize the numerous Defendants into four groups: 1) DISH Network LLC, NagraStar LLC, Bert Eichhorn, Emily Rinkel,[2] Jordan Smith, and Kevin Gedeon (the DISH/NagraStar Defendants); 2) DISH Network Corporation (DISH Corp. or DNC); 3) Toltec Investigations, LLC and its President and CEO, Michael Thomas Jaczewski (the Toltec Defendants); and, 4) former U.S. Attorney Rosa E. Rodriguez-Velez, former Assistant U.S. Attorney Jose Capo-Iriarte, Assistant U.S. Attorney Nicholas W. Cannon (the USAO Defendants) and Special Agents and employees of the Federal Bureau of Investigation Douglas Leff, Bradley Rex, Lance

---

[1] This is the second lawsuit arising out of the underlying events at issue. On August 25, 2020, a group of plaintiffs, including many of Plaintiffs here, filed a *Bivens* action against many of the same defendants. *See Quinones-Pimentel v. Cannon*, No. 3:20-cv-01443-JAW, 2022 U.S. Dist. LEXIS 48109, at *2-3 (D.P.R. Mar. 17, 2022). On March 17, 2022, the Court dismissed the *Bivens* action. *Id.* at *88. The plaintiffs appealed, and the Court of Appeals for the First Circuit affirmed the Court's dismissal on October 27, 2023. *Quinones-Pimentel v. Cannon*, 85 F.4th 63, 66-68 (1st Cir. 2023).

[2] In their Second Amended Complaint, Plaintiffs use the spelling, "Rinkle." *See, e.g.*, *Second Am. Compl.* ¶ 43. In their filings, however, the DISH/NagraStar Defendants use the spelling, "Rinkel." *See, e.g.*, *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel, and Jordan Smith's Mot. to Dismiss* at 1 (ECF No. 134). No doubt, Ms. Rinkel knows how to spell her own name, and the Court uses "Rinkel" throughout this order.

Lange, Kevin Pearson, Clay Rehrig, Juan Galarza, and Jason Lopez (the FBI Defendants) (collectively, the Federal Defendants).

Plaintiffs allege: 1) violations of the Racketeer Influenced and Corrupt Organizations Act (RICO); 2) a RICO conspiracy; 3) violations of the Computer Fraud and Abuse Act (CFAA); 4) violations of the Stored Communications Act (SCA); 5) violations of the Digital Millennium Copyright Act (DMCA); 6) violations of the Defend Trade Secrets Act (DTSA) by misappropriation of trade secrets; and 7) violations of the Puerto Rico Industrial and Trade Secrets Protection Act (PTSA) under the Uniform Trade Secrets Act (Law No. 80). *Second Am. Compl.* ¶¶ 124-202.

On October 31, 2022 and November 1, 2022, each of the four groups of Defendants filed a motion to dismiss the complaint. *Fed. Defs.' Mot. to Dismiss* (ECF No. 138) (*Defs.' Mot.*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Mot. to Dismiss* (ECF No. 134); *Def. DISH Network Corp.'s Mot. to Dismiss* (ECF No. 136); *Defs.' Toltec Investigations L.L.C. and Mike Jaczewski's Mot. to Dismiss* (ECF No. 137).

On December 5, 2022, Plaintiffs filed a response to the DISH/NagraStar Defendants' motion to dismiss. *Mot. in Resp. to Dish/NagraStar Defs.' Mot. to Dismiss* (ECF No. 147) (*Pls.' Opp'n to DISH/NagraStar Mot.*). On January 18, 2023, Plaintiffs responded to the Federal Defendants' motion. *Mot. in Resp. to the Fed. Defs.' Mot. to Dismiss* (ECF No. 153) (*Pls.' Opp'n*). On February 21, 2023, the Toltec Defendants withdrew a section of their motion to dismiss, *Unopposed Notice of Partial Withdrawal of Toltec Investigations L.L.C. and Mike Jaczewski's 12(b)(2) Mot. to*

Dismiss (ECF No. 163), and on February 27, 2023, Plaintiffs responded to the remainder of the Toltec Defendants' motion. *Mot. in Resp. to Toltec Investigations and Mike Jaczewski's Mot. to Dismiss* (ECF No. 167). On March 17, 2023, Plaintiffs responded to DISH Corp.'s motion. *Mot. in Resp. to Dish Network Corp.'s Mot. to Dismiss* (ECF No. 179).

Each group of Defendants filed a reply in support of its motion. *Fed. Defs.' Reply* (ECF No. 173) (*Defs.' Reply*); *DISH Network L.L.C., NagraStar LLC, Kevin Gedeon, Bert Eichhorn, Emily Rinkel and Jordan Smith's Reply* (ECF No. 164); *Defs. Toltec Investigations L.L.C. and Michael Jaczewski's Reply in Supp. of Rule 12(b)(6) Mot. to Dismiss* (ECF No. 185); *DISH Network Corp.'s Reply in Supp. of Its Mot. to Dismiss* (ECF No. 196).

Finally, Plaintiffs filed sur-replies opposing each motion. *Sur-Reply Mot. to Fed. Defs.' Reply Mot. to Pls.' Resp. to Fed. Defs.' Mot. to Dismiss, SAC* (ECF No. 190) (*Pls.' Sur-Reply*); *Sur-Reply to the Dish Network, LLC and NagraStar, LLC Reply Mot. to Pls.' Resp. to Defs.' Mot. to Dismiss SAC* (ECF No. 182); *Sur-Reply Mot. to the Toltec Investigations L.L.C. and Michael Jaczewski's Reply Mot. to Pls.' Resp. to Their Mot. to Dismiss SAC* (ECF No. 195); *Sur-Reply Mot. to Dish Network Corp.'s Reply Mot. to Pls.' Resp. to Mot. to Dismiss SAC* (ECF No. 199).

II. FACTS[3]

A. The Parties

In 2015 and 2016, Darwin Quinones-Pimentel and Victor Vega-Encarnacion founded Naicom Corporation and D&V IP Holdings, LLC to offer Internet Protocol Television (IPTV) services. The companies are structured such that D&V holds the proprietary "intellectual technology" created by Mr. Quinones, and Naicom licenses the technology from D&V to distribute television programming. *Second Am. Compl.* ¶ 63. Kiaras, LLC and Paylink, LLC are also joint ventures operated by Mr. Quinones and Mr. Vega. *Id.* ¶ 14. Kiaras is a human resources and time-and-attendance management company, and PayLink is a payroll processing company. *Id.* Both Kiaras and PayLink operate on the "PAYLINK AND KIARAS Cloud Network," another proprietary intellectual technology creation of Mr. Quinones. *Id.* ¶¶ 5-6. All four companies are corporations existing under the laws of the commonwealth of Puerto Rico with their places of business located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907. *Id.* ¶¶ 33-36.

DISH Network Corporation (DISH Corp.) was organized in 1995 as a corporation under the laws of the State of Nevada, started offering the DISH® branded pay-tv service in March 1996, and is the nation's third largest pay-tv

[3] Consistent with Federal Rule of Civil Procedure 12(b)(6), in describing the facts, the Court has relied upon the allegations in the Second Amended Complaint. *Foley v. Wells Fargo Bank, N.A.*, 772 F.3d 63, 68 (1st Cir. 2014); *Medina-Velázquez v. Hernández-Gregorat*, 767 F.3d 103, 108 (1st Cir. 2014) ("We examine whether the operative complaint states a claim for which relief can be granted when we construe the well-pleaded facts in the light most favorable to the plaintiffs, accepting their truth and drawing all reasonable inferences in plaintiffs' favor" (internal citation omitted)).

provider. *Id.* ¶ 37. DISH Network LLC (DISH LLC) was organized in 1987 as a Limited Liability Corporation under the laws of the state of Colorado. *Id.* ¶ 38.

NagraStar, LLC is a joint venture between DISH Corp. and Kudelski SA formed in 1998. *Id.* ¶ 39. NagraStar's focus is delivering and maintaining security solutions for satellite and Internet-based television systems and other connectivity initiatives in North America, and their mission also includes anti-piracy investigations and cooperation with law enforcement agencies. *Id.* Jordan Smith was at all relevant times a Manager of Field Security & Investigations and Senior Anti-Piracy Investigator for NagraStar. *Id.* ¶ 41. Bert Eichhorn and Emily Rinkel were Managers of Field Security & Investigations for NagraStar. *Id.* ¶¶ 42-43. Kevin Gedeon was a Manager of Fraud Investigations for NagraStar. *Id.* ¶ 44.

Toltec Investigations, LLC (Toltec) is a private investigative agency specializing in investigating the technology and distribution involved in IPTV systems, copyrights, patents, and "Trademark and Brand's Intellectual Property." *Id.* ¶ 40. Michael Thomas Jaczewski, a.k.a. Brian Parsons, was at all relevant times President and Chief Executive Officer of Toltec. *Id.* ¶ 45.

Rosa Emilia Rodriguez-Velez was at all relevant times the United States Attorney for the District of Puerto Rico. *Id.* ¶ 46. Jose Capo-Iriarte was an Assistant U.S. Attorney (AUSA) and head of the office's Criminal Division. *Id.* ¶ 47. Nicholas Cannon was an AUSA and Deputy Chief of the Cybercrimes Division. *Id.* ¶ 48.

Douglas Leff was at all relevant times Special Agent in Charge of the FBI's San Juan Division. *Id.* ¶ 49. Also in that division, Brad Rex was a Supervisory

Special Agent; Lance Lange, Kevin Pearson, and Clay Rehrig were Special Agents; Juan Galarza was a Computer Science Officer; and Jason Lopez was an Evidence Technician. *Id.* ¶¶ 50-55.

B. Naicom's Origins

Between 2002 and 2012, Mr. Quinones developed the intellectual technology, including the source code, underpinning the Paylink and Kiaras Cloud Workforce Management system and Naicom's IPTV services. *Id.* ¶ 5. The proprietary IPTV system was characterized as a Dynamic Internet Semantic Multicast Environment (DISME), which "enabled for the first time the broadcast of media via private networks and the internet, a new concept of IPTV service to distribute Live-Video Television Content (media) to residences, business, and primes customers." *Id.* ¶¶ 8-11.

By 2016, Mr. Quinones had completed all DISME technology alpha and beta tests and, alongside Mr. Vega, founded Naicom. *Id.* ¶ 12. Naicom is a network and internet communication platform that delivers live television, video on-demand content, internet, and wireless network services to subscribers worldwide. *Id.* Naicom also provides instant access to television shows, movies, and music/videos on-demand, and live sports and music events through Naicom's set-top box using IPTV and TV Everywhere (TVE) on any mobile device. *Id.*

Mr. Quinones and Mr. Vega registered Naicom as a closed corporation with the State Department of Puerto Rico and complied with all requirements as a legitimate IPTV business. *Id.* ¶ 66. Naicom also requested to manufacture its own brand of set-top boxes for end users through Informir LLC and acquired the programing licenses

to distribute on-demand content in the United States, Puerto Rico, and the U.S. Virgin Islands through worldwide television network companies. *Id.* ¶¶ 67-68. In 2017, Naicom became a member of the National Rural Telecommunications Cooperative (NRTC). *Id.* ¶ 68.

On January 6, 2017, Naicom submitted a request to the Apple Corporation to have its TV App added to Apple's AppStore. *Id.* ¶ 69. Apple's legal department requested that Naicom produce all licenses authorizing the distribution of programming to Naicom's subscribers via Naicom's TV App. *Id.* On February 16, 2017, Apple approved Naicom's App for inclusion in the Apple AppStore. *Id.* ¶ 70. In December 2017, Sam's Club approved Naicom to launch and distribute Naicom's IPTV set-top box in their retail stores. *Id.* ¶ 71.

C. Naicom's Information Security

Naicom went to great lengths to protect its intellectual technology. *Id.* ¶¶ 64-65. D&V IP Holdings and Naicom developed significant amounts of confidential and proprietary information, including non-public information relating to the DISME's source codes, patterns, formulas, algorithms, methods, and techniques; the technological vision for Naicom's IPTV content, distribution, marketing, servicing, research and development efforts and strategies; business and marketing performance strategies; financial data and business plans; technical data; customer development management programs; and subcontractor and vendor relationships (collectively, with the DISME, the Confidential Information or Naicom's Confidential Information). *Id.* ¶ 64.

To protect this information, Plaintiffs only installed on their servers, located at Naicom's Data Center Facility, what is known as a compiled executable. *Id.* ¶ 65. The entire system was installed with an operating system that allowed the hard drive to be encrypted and, to access the servers, an authorized employee would need to enter the secure data facility and provide a username and password. *Id.* The server is not exposed to the internet and could only be accessed from inside the facility. *Id.* The Confidential Information was also downloaded onto a hard disk and kept in a safe box. *Id.*

Plaintiffs took additional steps to safeguard their confidential information and proprietary data, including restricting employee access, requiring employees to execute non-disclosure agreements, imposing restrictions on remote access, and implementing encryption. *Id.* ¶¶ 72-76.

D. Negotiations with Claro Puerto Rico

In 2017, Naicom entered into negotiations with Claro Puerto Rico[4] to distribute Naicom set-top boxes to Claro customers. *Id.* ¶ 77. Claro represented to Naicom that it had approximately 320,000 internet subscribers who received only five megabytes and thus could not subscribe to Claro's IPTV services, which required sixty megabytes to upload programming. *Id.* ¶ 78. During negotiations, Naicom and Claro entered into a mutual non-disclosure agreement prior to discussing and analyzing business

[4] Presumably because Claro Puerto Rico is a well-known business in Puerto Rico, the Second Amended Complaint does not describe Claro Puerto Rico except by name. *See Second Am. Compl.* ¶ 68. According to Wikipedia, Claro Puerto Rico is the one of the largest telecommunications companies in Puerto Rico. *See Claro P.R.*, WIKIPEDIA (updated Oct. 14, 2023), *https://en.Wikipedia.org/wiki/Claro_Puerto_Rico.*

information and the contents of the resellers' agreement. *Id.* ¶ 79. Claro's Product Development Officer, Anibal Rios, projected that the Claro-Naicom business alliance would bring in over $10,000,000 in monthly gross revenue for the first year and over $13,000,000 for the second year, only taking into account Claro's corporate and residential subscribers in Puerto Rico. *Id.* ¶ 80. Naicom projected that the Claro-Naicom alliance would add 100,000 new corporate subscribers, plus another 150,000 residential subscribers, bringing in projected monthly gross sales of $9,000,000 in the first year and $12,000,000 in the second year. *Id.* ¶ 81.

Claro had an existing contract with DISH Network Satellite TV, whereby DISH Network provided TV programming to Claro's internet subscribers who could not subscribe to Claro's IPTV services. *Id.* ¶ 82. The Naicom deal represented a cancellation threat to DISH Network's contract with Claro. *Id.* Claro was also considering shutting down its IPTV business division due to loss of revenue. *Id.* During the negotiations for the Claro-Naicom deal, Carlos Garcia, Claro's IPTV business manager, became privy to information that the Claro-Naicom deal would leave him jobless if Claro opted to shut down its IPTV division, which he managed. *Id.* ¶ 83. Mr. Garcia alerted DISH Network that the Claro-Naicom IPTV deal would lead to cancellation of the DISH contract with Claro, which the Plaintiffs allege led to "great animosity" between DISH Network and Naicom. *Id.* ¶ 84. On August 14, 2018, after a year of meetings between Naicom and Claro, Claro pulled out of negotiations without notice. *Id.* ¶ 85. Plaintiffs believe the DISH Network

Defendants advised Claro to withdraw because the FBI was investigating Naicom and its founders. *Id.* ¶ 86.

E. The DISH Network Investigation

On August 7, 2017, the DISH/NagraStar Defendants and DISH Corp. instructed the Toltec Defendants to purchase two Naicom TV set-top box receivers so that the Defendants[5] could reverse engineer Plaintiffs' intellectual technology. *Id.* ¶ 87. The Defendants conducted "sniffing" to determine the direction of Naicom TV traffic and locate Naicom's facility. *Id.* The defendants also used sniffing to attack and penetrate Naicom's servers and computers, monitoring content and capturing information on the network under the supervision of the Federal Defendants. *Id.* One of the two set-top box receivers was maintained by the DISH/NagraStar Defendants, the other by the Toltec Defendants. *Id.* ¶ 88. Both receivers were used for the attacks on Naicom's data center servers. *Id.*

Mr. Jaczewski purchased the two set-top boxes from Naicom under the false name of "Brian Parsons," and he provided false contact information. *Id.* ¶ 89. According to the Defendants, their investigation revealed that the receiver provided access to approximately forty-three channels, including Disney, TBS, ESPN, CNN, HBO, Showtime, and Cinemax. *Id.* ¶ 90. The Defendants downloaded the Naicom TV App through the Apple AppStore, which provided access to approximately forty-

[5] Plaintiffs often refer in the Second Amended Complaint to the "Association in Fact defendants." *See, e.g., Second Am. Compl.* ¶ 87. As the Court interprets Plaintiffs' complaint, this term refers to all Defendants collectively. *See id.* ¶¶ 17, 62 (listing all the Defendants as together "form[ing] an Association in Fact").

two channels, and tested Naicom TV several times to determine whether it was providing DISH programming. *Id.* The tests revealed no DISH content. *Id.*

The Defendants also contacted several media companies to inquire into whether Naicom had the appropriate licensing contracts to distribute its programming. *Id.* ¶ 91. On each occasion, the investigators were informed that Naicom was authorized to distribute the network's content. *Id.* The investigators also discovered that Naicom's TV distribution technology was a threat to DISH Network and Sling TV, representing future competition for subscribers in Puerto Rico and the United States. *Id.* ¶ 92.

The DISH/NagraStar Defendants informed the other Defendants that they could not penetrate Naicom's Data Center computers and servers remotely, and thus direct, physical access would be required to extract Naicom's intellectual property. *Id.* ¶ 93. They knew that by entering the data center and shutting down the computers and servers, they would be able to bypass Naicom's security measures and access the internal hard drive. *Id.* ¶ 94.

According to Naicom, the Defendants knew that the intellectual property was extremely valuable and worth obtaining by any means necessary to advance their own television programming distribution system, and the Defendants conspired to misappropriate the technology for economic advantage. *Id.* ¶ 95.

The DISH/NagraStar Defendants thereafter filed a complaint with the Federal Defendants alleging that Naicom was running an IPTV pirate operation. *Id.* ¶ 98. Plaintiffs allege that the motive behind the complaint was to secure NagraStar and

DISH Network's participation in a search of Naicom's Data Center and the seizure of Naicom's computers, servers, and other hardware containing Naicom's intellectual property and trade secrets, under the ruse of assisting the Federal Defendants in discovering incriminating evidence. *Id.* Acquiring this information has given the DISH/NagraStar Defendants a competitive advantage over Naicom. *Id.* ¶ 99.

F. Execution of the Search Warrants

1. The First Search of Naicom's Data Center

On August 27, 2019, the Federal Defendants applied for two search warrants: one for Naicom Corporation located at Building Centro de Seguros, 701 Ponce de Leon, Suite 208, San Juan, Puerto Rico 00907, and the other for Naicom's Data Center located at Villa Fontana, 4SS N2 Via Josefina, Carolina, Puerto Rico. *Id.* ¶¶ 19, 33, 105. Plaintiffs allege that the search warrants were "issued under illegal and unlawful means" because the Federal Defendants provided affidavits they knew to contain false and perjured information. *Id.* ¶ 20.

On August 27, 2019, the Federal and DISH/NagraStar Defendants executed the warrants, with the DISH/NagraStar Defendants "acting as federal agents." *Id.* ¶ 21. They seized documents, hard drives, and thumb drives, and downloaded data from the computers and servers containing Plaintiffs' Confidential Information. *Id.* Plaintiffs allege that the Defendants knew from their investigation prior to the searches that Naicom was authorized to distribute its programming and was not pirating content. *Id.* ¶ 101. The Defendants also allegedly knew that the evidence collected in the Federal Defendants' investigative files "negated any criminal

wrongdoing that Naicom's founders were committing the crimes charged in the search and seizure warrant affidavit and application." *Id.* ¶ 102.

At the conclusion of the August 27, 2019 search, the Federal Defendants "learned that Naicom TV counted with all the programming distribution contract and agreements"[6] and instructed Mr. Quinones and Mr. Vega to report to the FBI offices with their licensing contracts for an interview. *Id.* ¶ 103. This interview took place with the Federal Defendants sitting at one table and the DISH/NagraStar Defendants sitting at another table, allegedly posing as federal agents. *Id.* ¶ 104. The Defendants questioned Mr. Quinones about how Naicom acquired the IPTV distribution contracts and the technology used to distribute the programing. *Id.* They also inspected Naicom's contracts with content providers, which contained trade/business secrets and confidential information regarding DISME technology. *Id.*

2. The Second Search of Naicom's Data Center

On August 29, 2019, U.S. Attorney Rodriguez-Velez and AUSAs Capo-Iriarte and Cannon instructed FBI Agents Lange and Pearson to return to Naicom's data center with DISH/NagraStar Defendants Smith, Gedeon, and Eichhorn. *Id.* ¶ 105. Naicom alleges that the USAO Defendants ordered this search despite knowing beforehand that Naicom was a legitimate business and there was no probable cause for continued investigation. *Id.* Without obtaining new warrants, the Defendants again entered Naicom's Data Center, performed password resets, and installed "pen

[6] Here, the Court quotes the text in the Second Amended Complaint. *Second Am. Compl.* ¶ 103. In the context of this sentence, the meaning of the verb, "counted," is unclear. It would make more sense if the sentence used "complied with," rather than "counted." Whichever verb is correct, however, makes no difference in the Court's ruling on the motion to dismiss.

drives and other electronic instruments" to bypass security measures and download and seize Naicom's Confidential Information. *Id.* ¶¶ 22, 106. The agents used keys taken from Naicom's offices to enter Naicom's Data Center. *Id.* ¶ 105.

During the search, Agent Pearson contacted Naicom employee Jaime Echevarria and ordered him to come to the Data Center, as Agent Pearson wanted to speak with him, Mr. Quinones, and Mr. Vega. *Id.* ¶ 107. Upon arriving at the Data Center, Mr. Quinones observed Agents Lange and Pearson allowing Mr. Smith, Mr. Gedeon, and Mr. Eichhorn to access Naicom's Data Center computers, servers, and other hardware equipment without authorization from Naicom. *Id.* ¶ 108.

During the search, Agents Pearson and Lange pressured Mr. Quinones to sign a hold-harmless document accepting that he had run a pirate operation in the past so that they could close the case. *Id.* ¶ 109. Otherwise, they threatened that they would shut down the Data Center operation. *Id.* Mr. Quinones refused, despite Agents Pearson and Lange imploring him to sign the document. *Id.* ¶ 110.

Sometime thereafter, Mr. Vega arrived and, upon entering the Data Center, asked Agents Pearson and Lange if they had another search warrant to enter and search the Data Center. *Id.* ¶ 111. Agent Lange represented to Mr. Vega that the search warrants gave him ten days to come in and out and search the Data Center. *Id.* Mr. Vega told Agent Lange that Agent Lange was violating the United States Constitution and federal law. *Id.*

Mr. Vega thereafter informed Agents Pearson and Lange that he had discovered via LinkedIn that the alleged FBI experts who executed the search and

interrogated Mr. Quinones and him at the FBI offices were Kevin Gedeon, investigator for DISH Network, and Jordan Smith, Bert Eichhorn, and Emily Rinkel, investigators for NagraStar. *Id.* ¶ 112. Mr. Vega questioned Agents Lange and Pearson as to why the FBI brought in his competition to search, inspect, and photograph private documents and allowed them access to computers and servers containing trade secrets, code sources, and business and intellectual property belonging to Naicom. *Id.* ¶ 113. Mr. Vega called his attorney and told him about the second search. *Id.* ¶ 114. After speaking with Agent Lange, the FBI agents and DISH/NagraStar investigators shut down Naicom's business operation and left the premises. *Id.*

G. The Demand for the Return of Property Under Rule 41(g)

On September 6, 2019, Plaintiffs filed a motion to demand the return of seized property under Rule 41(g) of the Federal Rules of Criminal Procedure. *Id.* ¶ 115. The District Court granted Plaintiffs' Rule 41(g) motion on November 5, 2019, noting that the Government had waived objections to the court's Report & Recommendation. *Id.* ¶¶ 116-17.

H. Plaintiffs' Alleged Harms

Plaintiffs allege that the criminal investigation caused significant damage to their business reputation and unfairly enriched their competitors. *Id.* ¶¶ 118-19. They allege that prior to the execution of the search warrants, they had a great reputation and were about to close on a $15,000,000 investment deal, but investors pulled out upon learning Naicom was under criminal investigation. *Id.* ¶¶ 120-21. Plaintiffs also allege that Naicom was about to close a multimillion-dollar deal with

Claro when Claro learned of the FBI's investigation and pulled out of negotiations. *Id.* ¶ 122. Plaintiffs say they have lost subscribers because of negative publicity resulting from the investigation and that the Defendants' intrusion into Naicom's Data Center computers, servers, and equipment caused damage leaving subscribers without TV programming services for several weeks and costing more than $500,000 to repair. *Id.* ¶ 123.

I. Plaintiffs' Causes of Action

Plaintiffs bring seven counts. Count One alleges that the Defendants violated RICO by forming an association in fact to advance the criminal objective of stealing Plaintiffs' intellectual property and trade secrets by committing mail and wire fraud, among other crimes. *Id.* ¶¶ 124-53.

Count Two alleges that the Defendants engaged in a RICO conspiracy by conspiring to plan and execute the scheme outlined in Count One. *Id.* ¶¶ 154-57.

Count Three alleges that the Defendants violated the CFAA by accessing Naicom's computer systems without authorization or in excess of authorization and obtaining and using valuable information from those computers. *Id.* ¶¶ 158-68.

Count Four alleges that the Defendants violated the SCA by "willfully and intentionally access[ing] without authorization a facility which operates servers, encoders, computers, and telecommunications systems and technology, by electronically transmitting communications involved in Webservers, Email-Servers, Carrier Grade Routers which interconnected with local ISP providers through Border Gateway Protocols (BGP) in exchanging routing information between autonomous systems." *Id.* ¶¶ 169-75.

Count Five alleges that the Defendants violated the DMCA by illegally obtaining Plaintiffs' copyright-protected software programs, documents, confidential information, and research. *Id.* ¶¶ 176-84.

Count Six alleges that the Defendants violated the DTSA by stealing Plaintiffs' trade secrets, including DISME technology, intellectual property, and other confidential information. *Id.* ¶¶ 185-94.

Finally, Count Seven alleges that the Defendants misappropriated Plaintiffs' trade secrets in violation of the PTSA. *Id.* ¶¶ 195-202.

III. THE PARTIES' POSITIONS

A. The Federal Defendants' Motion to Dismiss

The Federal Defendants move to dismiss all counts of the Second Amended Complaint. *Defs.' Mot.* at 1-39.

The Federal Defendants begin by arguing that the individual capacity statutory claims should be dismissed for failure to state a claim on which relief may be granted because qualified immunity shields federal employees from individual capacity damages suits unless they violate clearly established constitutional or statutory rights. *Id.* at 8. They contend that because, in their view, Plaintiffs fail to allege any statutory violations, qualified immunity bars suit. *Id.* The Federal Defendants submit that "[o]nce the conclusory and speculative allegations and threadbare recital of elements of a cause of action are set aside, it is apparent that the plaintiffs' lengthy complaint cannot support any of the claims it advances against the Federal Defendants." *Id.* at 9. They add that "[t]he plaintiffs similarly fail to specify the particular conduct of each Federal Defendant that supposedly forms the

basis for liability. Instead, the complaint alleges collective legal wrongs," which "is especially improper when the defendants are public officials." *Id.* at 10.

Turning to the statutory claims, the Federal Defendants assert that "plaintiffs rely on broad, conclusory, allegations of wrongdoing that fail to establish any of the four requisite elements of a civil RICO claim." *Id.* at 11. In their view, Plaintiffs do not plausibly allege that the Federal Defendants joined with other Defendants to form an enterprise and directed the operations of the purported enterprise, the alleged pattern of racketeering activity is deficient, and the limited breadth, duration, and purpose of the supposed racketeering activity do not establish the pattern required to sustain a RICO claim. *Id.*

The Federal Defendants submit that the Second Amended Complaint "lacks well-pleaded allegations showing that the Federal Defendants participated in any association-in-fact 'enterprise.'" *Id.* at 13. Furthermore, they contend that "plaintiffs also do not distinguish the alleged enterprise from their allegations of racketeering activity as RICO requires." *Id.* at 14. Specifically, the complaint "supposes an enterprise that exists exclusively to obtain the plaintiffs' confidential information" and "[b]y conceiving an enterprise in such narrow terms, the plaintiffs fail to plausibly allege a RICO enterprise." *Id.*

The Federal Defendants also assert that "[t]he plaintiffs make no allegations sufficient to connect the Federal Defendants to the conduct of the supposed enterprise's affairs" and thus "the complaint does not plausibly allege that the Federal Defendants were conducting the affairs of some association-in-fact enterprise

with the other defendants instead of their own federal agencies' official business." *Id.* at 14-15. They add that "[t]he plaintiffs' allegations are all the more implausible given an obvious alternative explanation for the searches, namely that the Federal Defendants pursued a lawful criminal investigation." *Id.* at 15 (citation and internal quotation marks omitted). Ultimately, they offer that "the RICO claims against each Federal Defendant fail both for want of an 'enterprise' and lack of plausible allegations that any particular Federal Defendant participated in the posited enterprise." *Id.* at 16.

Next, the Federal Defendants argue that "Plaintiffs fail to plausibly allege that the Federal Defendants engaged in a pattern of racketeering activity." *Id.* at 17. They submit that "[t]he plaintiffs' RICO theory here relies for its predicate acts on supposed mail and wire fraud, and allegations of misappropriation of trade secrets" but "the plaintiffs cannot plausibly allege the Federal Defendants committed the supposed predicate offenses based on the FBI's execution of a search warrant at Naicom's San Juan office and its data center." *Id.* at 17-18. Additionally, they offer that "[b]eyond failing to coherently allege the minimum predicate acts, the plaintiffs fail to 'allege facts linking each [Federal] defendant to the grounds on which that particular defendant is potentially liable' for the supposed pattern of racketeering activity." *Id.* at 19 (alteration in original) (quoting *Redondo Waste Sys. v. López-Freytes*, 659 F.3d 136, 140 (1st Cir. 2011)).

The Federal Defendants' final argument against the RICO claim is that the alleged scheme lacks the requisite continuity because Plaintiffs "allege a narrow

scheme directed exclusively at the acquisition of their intellectual property and trade secrets" and "[t]he allegations here describe no risk of the alleged activity continuing." *Id.* at 20.

Briefly addressing the RICO conspiracy claim, the Federal Defendants claim that the Plaintiffs' failure to plead a substantive RICO claim inherently defeats the conspiracy claim. *Id.* at 20-21.

Next, the Federal Defendants address the CFAA claim, contending that it fails as a matter of law "because the CFAA does not prohibit lawfully-authorized investigative activity of federal law enforcement agencies" and "the government had a warrant to search the plaintiffs' computers." *Id.* at 21. Moreover, they submit that "[t]he Federal Defendants also did not 'access' the plaintiffs' computers, and the plaintiffs do not allege a compensable loss or damage caused by the Federal Defendant's actions." *Id.*

Regarding the SCA claim, the Federal Defendants argue that electronic materials accessed during the raids were not "electronic communications" as defined and protected by the Act. *Id.* at 26-28. They submit further that none of the Federal Defendants accessed Plaintiffs' computers, the Federal Defendants lacked the requisite state of mind for liability under the SCA and, in any event, the SCA provides that good faith reliance on a warrant is a complete defense. *Id.* at 28-30.

The Federal Defendants stake out similar positions on the DMCA claim, contending that if anyone engaged in copyright circumvention it was the

DISH/NagraStar Defendants alone and, regardless, the statute protects authorized law enforcement activity. *Id.* at 30-32.

Regarding the DTSA claim, the Federal Defendants assert that Plaintiffs have failed to adequately plead the existence of a trade secret and—again—the statute protects authorized law enforcement activity. *Id.* at 32-35.

The Federal Defendants then pivot back to immunity, contending that the Westfall Act provides for absolute immunity for all Federal Defendants on the PTSA claim, and absolute prosecutorial immunity shields the USAO Defendants for their prosecutorial acts. *Id.* at 35. They submit that the Westfall Act provides that tort claims against federal employees acting in the scope of their employment must be brought under the Federal Tort Claims Act (FTCA), which mandates the immediate substitution of the United States as the defendant. *Id.* at 35-36. The Federal Defendants argue that the United States must be substituted as defendant and the claim must then be dismissed because Plaintiffs have not complied with the FTCA's procedural requirements. *Id.* at 36.

Finally, regarding prosecutorial immunity, the Federal Defendants submit that the USAO Defendants are absolutely immune from suit because their conduct was "intimately associated with the judicial phase of the criminal process." *Id.* at 37 (quoting *Imbler v. Pachtman*, 424 U.S. 409, 430 (1976)).

B. Plaintiffs' Opposition

Plaintiffs oppose the Federal Defendants' motion by first insisting that the "individual capacity statutory claims state a claim upon which relief could be granted, therefore, the Federal Defendants are not entitled to qualified immunity from

Plaintiffs' RICO claims." *Pls.' Opp'n* at 10. They submit that the Second Amended Complaint alleges against the Federal Defendants "criminal and civil violations [that] were clearly established and prohibited at the time they committed the crime" and thus they are not entitled to qualified immunity. *Id.* at 12-13.

Plaintiffs further acknowledge that the Attorney General's designee has certified, pursuant to the Westfall Act, that the Federal Defendants were acting within the scope of their employments. *Id.* They assert, however, that the Federal Defendants did not act within the scope of their official duties and that if the Court agrees it must re-substitute the Federal Defendants. *Id.* at 68-69. Similarly, Plaintiffs contend that the USAO Defendants are not entitled to absolute prosecutorial immunity because their conduct "violated clear and established criminal and civil laws" and was not in furtherance of their protected prosecutorial duties.[7] *Id.* at 71-73.

Turning to the RICO counts, Plaintiffs submit that they have pleaded "a colorable RICO claim on the facts" because "they have plead[ed] enough facts in the [Second Amended Complaint] giving defendants a fair notice of what there is, and the grounds upon which they rest." *Id.* at 16-17. They add that they also "have pleaded a colorable RICO enterprise on the facts." *Id.* at 18-20.

[7] Plaintiffs also argue that sovereign immunity does not apply to their RICO claims, although the Federal Defendants did not invoke sovereign immunity in their motion to dismiss. *Pls.' Opp'n* at 15-16. They submit that their claims "were not brought against the United States, but against specific federal official/agent[] defendants, in their individual and personal capacities, for criminal actions indictable under RICO, falling outside their scope of employment, and beyond their statutory authority," and thus Plaintiffs "are allowed to prosecute under equitable civil remedies of the United States laws." *Id.* at 16.

Plaintiffs further contend that they have sufficiently pleaded "conduct of a criminal enterprise that is separate and apart from the conduct of defendants' own affairs." *Id.* at 20. In their view, the three required elements for establishing a RICO enterprise are: (1) "an ongoing organization, formal or informal," (2) that "the various associate[s] function as a continuing unit," and (3) that the enterprise exists "separate and apart from the pattern of activity in which it engages." *Id.* at 21 (quoting *United States v. Turkette*, 452 U.S. 576, 583 (1981)). Plaintiffs assert, however, that while they "will ultimately need to establish each of these factors, at this early juncture it is sufficient to merely [] allege the existence of an association-in-fact enterprise." *Id.* (citing *Pappa v. Unum Life Ins. Co. of Am.*, No. 3:07-cv-0708, 2008 U.S. Dist. LEXIS 21500, at *29-30 (M.D. Pa. Mar. 18, 2008)). They add that it is reasonable to infer from the complaint that "the Association in Fact defendants comprised by the Federal and Dish/Nagrastar defendants, functioned as a continuing unit and had an ascertainable structure distinct from that inherent in the conduct of a pattern of racketeering activity." *Id.* at 22.

Plaintiffs argue that they have established a pattern of racketeering activity because they have "pleaded that the Association in Fact defendants committed over 30 racketeering acts ranging from Mail and Wire fraud to theft of trade secrets, in a period of two years which began in July 2017 and ended in August 2019." *Id.* at 25. In their view, "[t]hese facts satisfied the closed period of repeated conduct" and there are also "allegations of a threat of continued activity, in reference to the Dish Network and Nagrastar corporation joint venture." *Id.* at 25-26. Plaintiffs submit further that

they have pleaded a viable RICO conspiracy claim and that—contrary to the Federal Defendants' assertions—pleading an actionable substantive RICO claim is not a prerequisite for a RICO conspiracy claim. *Id.* at 27-29.

Plaintiffs next turn to their CFAA claim, beginning by addressing the Federal Defendants' position that any computer intrusions were protected lawfully authorized investigative activity. *Id.* at 30. Plaintiffs rejoin that the Defendants' conduct is not covered by this exception because "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Id.* They contend that the "search warrant contained materially false representations and perjured testimony" and ultimately lacked probable cause. *Id.* at 31. Plaintiffs submit further that the "alleged initial probable cause dissipated with the first search warrant execution" and thus the second search was "illegal and warrantless." *Id.* at 35.

Plaintiffs go on to argue that the "affidavit in support of the search warrant was defective on its face." *Id.* at 36. They contend that their computer systems were protected under the SCA, the Federal Defendants' "conclusory" statements were insufficient to justify a search, and the search ultimately did not comply with the SCA. *Id.* at 37-38. According to Plaintiffs, the Federal Defendants did not "seek authorization from the Magistrate to bring Plaintiffs' competitors, the Dish/Nagrastar defendants, to execute the search warrant," and although Plaintiffs concede that 18 U.S.C. § 3105 "allowed the aid of private parties," they rejoin that "the statute clearly prohibited the executing officer from bringing to the search a

party which had another interest, profit, or other marketplace incentive." *Id.* at 41. Plaintiffs submit further that "the Federal defendants cannot raise at this stage a legal defense which the Federal defendants abandoned when they did not oppose the Motion for Return of Property under Rule 41(g) proceedings." *Id.* at 43.

After concluding that the searches were generally unlawful, Plaintiffs return to the specifics of their CFAA claim. They offer that they have established each element of a CFAA violation and—contrary to the Federal Defendants' assertions—the fact that only the DISH/NagraStar Defendants actually intruded on Plaintiffs' computer systems is irrelevant because the Federal Defendants are responsible "under a conspiratorial theory of liability." *Id.* at 45-51.

Plaintiffs make similar arguments in support of their remaining claims. For the SCA claim, they submit that they have established each element of a SCA violation and reiterate that the search was not legally authorized. *Id.* at 52-60. In support of their DMCA claim, they "submit that for the same factual and legal reasons argued above, the Federal defendants also violated the Digital Millennium Copyright Act." *Id.* at 61. Plaintiffs again assert that the searches were not legally authorized and the Federal Defendants are liable for the DISH/NagraStar Defendants' conduct during the searches. *Id.* at 60-61.

Finally, turning to their trade secrets claims, Plaintiffs reiterate once more that the searches were not legally authorized and submit that the complaint adequately describes the trade secrets allegedly misappropriated by the Defendants.

Id. at 62-66. Plaintiffs conclude by asking the Court to deny the Federal Defendants' Motion to Dismiss in its entirety. *Id.* at 74.

C. The Federal Defendants' Reply

In reply, the Federal Defendants offer that "plaintiffs base their claims on allegations that are conclusory, collective, and speculative" and "[f]or that reason, and because the Federal Defendants are shielded by both absolute and qualified immunity, the Second Amended Complaint fails to state claims on which relief may be granted." *Defs.' Reply* at 1.

The Federal Defendants begin by comparing Plaintiffs' suit to *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), and *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007), and asserting that the "complaint relies on conclusory allegations to support the claims of wrongdoing, and none of its allegations plausibly support the inferences needed to sustain the plaintiffs' various statutory claims." *Id.* at 2-4.

They next contend that "[t]he plaintiffs are also incorrect that 'at this early juncture it is sufficient to merely allege the existence of an association-in-fact enterprise' to support their RICO claim." *Id.* at 5 (quoting *Pls.' Opp'n* at 21). The Federal Defendants add further that Plaintiffs have not plausibly alleged the existence of an association in fact, "that any of the Federal Defendants adopted and acted with the purpose of stealing their intellectual property," or "what benefit they gained from doing so." *Id.* at 5-6. Nor, in their view, do Plaintiffs "explain how the supposed association-in-fact enterprise functioned as a continuous unit." *Id.* at 7. Moreover, the Federal Defendants contend that "[t]he plaintiffs also fail to address

the Federal Defendants' lack of control over the alleged enterprise or participation in either its operation or management." *Id.*

Turning to the alleged pattern of racketeering activity, the Federal Defendants assert that Plaintiffs' response "is silent as to the predicate act allegations not complying with Rule 8 or Rule 9 pleading standards or describing adequately the Federal Defendants' involvement in Dish Network's supposed trade secret theft scheme." *Id.* at 8-9. In response to Plaintiffs' contention that an actionable substantive RICO claim is not a prerequisite for a RICO conspiracy claim, they rejoin that "First Circuit precedent clearly holds otherwise." *Id.* at 10 (citing *Efron v. Embassy Suites (P.R.), Inc.*, 223 F.3d 12, 21 (1st Cir. 2000)).

The Federal Defendants go on to argue that "Plaintiffs fail to overcome the search warrants' validity," characterizing Plaintiffs' allegations of perjury as conclusory and contending that they have failed to rebut key evidence supporting the search warrants. *Id.* at 10-14. The Federal Defendants add that their willingness to later return the seized property does not imply the invalidity of the search warrants or any other Fourth Amendment violation. *Id.* at 14-16.

For the remainder of Plaintiffs' claims, the Federal Defendants reject Plaintiffs' contentions that the searches were not legally authorized. *Id.* at 16-21. Regarding the CFAA claim, they submit that "plaintiffs' CFAA conspiracy claim suffers from the same pleading deficiencies as does the RICO conspiracy claim." *Id.* at 16. For the SCA claim, they offer that Plaintiffs' opposition "confuse[s] an SCA disclosure order with the traditional search warrant under the Federal Rules of

Criminal Procedure that the government, in fact, used to search the plaintiffs' offices and that was the subject of the plaintiffs' Rule 41(g) proceedings." *Id.* at 18. Furthermore, they assert that "the government appropriately opted for a traditional search warrant in this case because it sought to seize evidence of the plaintiffs' piracy operation rather than to require the plaintiffs to disclose certain electronic communications." *Id.*

On the DMCA claim, the Federal Defendants reiterate that it must fail because "[t]he Second Amended Complaint's allegations do not attribute circumvention conduct directly to any Federal Defendant. Nor do the Plaintiffs' allegations overcome the statute's broad law enforcement exception." *Id.* at 19. Similarly, they contend that the DTSA claim should be dismissed because "the plaintiffs rely on broad assertions that simply recite the elements of a DTSA claim, and because they do not address the statutory exemption applicable to the Federal Defendants' law enforcement actions in this matter." *Id.* at 20-21.

Finally, the Federal Defendants reject Plaintiffs' Westfall Act argument, asserting that they are protected because they acted within the scope of their employment and "[w]hether an employee acted in the scope of office or employment does not depend on whether his or her alleged actions can be characterized as tortious or even criminal." *Id.* at 21-23. Likewise, they reiterate that the USAO defendants are entitled to absolute prosecutorial immunity. *Id.* at 23-24.

D. Plaintiffs' Sur-Reply

In their sur-reply, Plaintiffs contend that: the Federal Defendants' Reply did not contribute anything not already discussed in their motion to dismiss; Plaintiffs

have met or exceeded the required pleading standard for each claim; and, the Federal Defendants have forfeited any "Fourth Amendment issue" relating to the search warrants or searches. *Pls. Sur-Reply* at 1-13.

IV. LEGAL STANDARD

Federal Rule of Civil Procedure 12(b)(6) requires dismissal of a complaint that "fail[s] to state a claim upon which relief can be granted." FED. R. CIV. P. 12(b)(6). To state a claim, a complaint must contain, among other things, "a short and plain statement of the claim showing that the pleader is entitled to relief." FED. R. CIV. P. 8(a)(2). In other words, a complaint must contain "sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 570). A claim is facially plausible when "the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* (citing *Twombly*, 550 U.S. at 556). Plausible means "'something more than merely possible' or 'merely consistent with a defendant's liability.'" *Germanowski v. Harris*, 854 F.3d 68, 71-72 (1st Cir. 2017) (internal citation omitted) (quoting *Schatz v. Republican State Leadership Comm.*, 669 F.3d 50, 55 (1st Cir. 2012)); *Ocasio-Hernández v. Fortuño-Burset*, 640 F.3d 1, 11 (1st Cir. 2011)). This is a "'context-specific' job that compels [judges] 'to draw on' [their] 'judicial experience and common sense.'" *Schatz*, 669 F.3d at 55 (quoting *Iqbal*, 556 U.S. at 679).

This is a "two-step analysis." *Cardigan Mountain Sch. v. N.H. Ins. Co.*, 787 F.3d 82, 84 (1st Cir. 2015). "First, the court must distinguish 'the complaint's factual allegations (which must be accepted as true) from its conclusory legal allegations

(which need not be credited).'" *García-Catalán v. United States*, 734 F.3d 100, 103 (1st Cir. 2013) (quoting *Morales-Cruz v. Univ. of P.R.*, 676 F.3d 220, 224 (1st Cir. 2012)); *see also Schatz*, 669 F.3d at 55 (stating that a court may "isolate and ignore statements in the complaint that simply offer legal labels and conclusions or merely rehash cause-of-action elements"). "Second, the court must determine whether the factual allegations are sufficient to support 'the reasonable inference that the defendant is liable for the misconduct alleged.'" *García-Catalán*, 734 F.3d at 103 (quoting *Haley v. City of Boston*, 657 F.3d 39, 46 (1st Cir. 2011)).

In ruling on a motion to dismiss, a court may properly take into account four types of documents outside the complaint without converting the motion into one for summary judgment: (1) documents of undisputed authenticity; (2) documents that are "official public records"; (3) documents that are "central" to a plaintiff's claim; and (4) documents that are sufficiently referenced in the complaint. *Watterson v. Page*, 987 F.2d 1, 3 (1st Cir. 1993). Here, the Second Amended Complaint refers to applications for search warrants. *See, e.g.*, *Second Am. Compl.* ¶¶ 18-21. The parties have not placed before the Court the search warrants themselves or the orders approving the warrants, but in ruling on this motion to dismiss, the Court has considered the parties' unchallenged characterizations of the timing and content of those warrants.

V. DISCUSSION

A. Absolute Prosecutorial Immunity

As a threshold matter, the Court evaluates the Federal Defendants' claim that the USAO Defendants are entitled to absolute prosecutorial immunity.

1. Caselaw

Immunity is "defined by the functions it protects and serves, not by the person to whom it attaches." *Acevedo-Garcia v. Vera-Monroig*, 204 F.3d 1, 8 (1st Cir. 2000) (internal quotation omitted). "[T]he official seeking absolute immunity bears the burden of showing that such immunity is justified for the function in question." *Burns v. Reed*, 500 U.S. 478, 486 (1991). There is a "presumption . . . that qualified rather than absolute immunity is sufficient to protect government officials in the exercise of their duties." *Id.* at 486-87. Prosecutors are absolutely immune from suit for monetary damages under § 1983 for conduct that is "intimately associated with the judicial phase of the criminal process." *Imbler v. Pachtman*, 424 U.S. 409, 430-31 (1976).

In *Buckley v. Fitzsimmons,* the Supreme Court reiterated the view expressed in *Burns* that absolute immunity does not extend to all actions by a prosecutor. 509 U.S. 259, 273 (1993) (citing *Burns*, 500 U.S. at 494-96). The *Buckley* Court refused to accord absolute immunity to "[a] prosecutor's administrative duties and those investigatory functions that do not relate to an advocate's preparation for the initiation of a prosecution or for judicial proceedings." *Id.* The Supreme Court further observed that in *Imbler* it "did not attempt to describe the line between a prosecutor's acts in preparing for those functions, some of which would be absolutely immune, and his acts of investigation or 'administration,' which would not." *Id.* at 270.

The caselaw provides examples of conduct that is and is not absolutely immune. In *Burns*, the Supreme Court concluded that prosecutors are not entitled to absolute immunity for the advice they give to the police, but they are entitled to

absolute immunity for participating in a probable cause hearing. 500 U.S. at 489-96. In *Buckley*, the Supreme Court rejected the petitioner's argument that absolute immunity extended "only to the act of initiation itself and to conduct occurring in the courtroom." 509 U.S. at 272. It restated *Imbler*'s conclusion that absolute immunity includes "actions preliminary to the initiation of a prosecution and actions apart from the courtroom." *Id.* (quoting *Imbler*, 424 U.S. at 431 n.33). The *Buckley* Court distinguished between actions a prosecutor takes as an advocate, ranging from evaluating evidence for prosecution to the prosecution itself, and actions a prosecutor takes as an investigator, such as "searching for the clues and corroboration" or planning and executing "a raid on a suspected weapons cache." *Id.* at 273-74. Summarizing its prior caselaw, the *Buckley* Court also clarified that "appearing before a judge and presenting evidence in support of a motion for a search warrant involved the prosecutor's 'role as advocate for the State,'" *id.* at 271 (quoting *Burns*, 500 U.S. at 491), and that "issuance of a search warrant is a judicial act . . . 'intimately associated with the judicial phase of the criminal process.'" *Id.* at 271 (quoting *Burns*, 500 U.S. at 492).

2. Analysis

The Federal Defendants submit that the USAO Defendants are entitled to absolute immunity because they were acting as advocates when they submitted the search warrant applications, and Plaintiffs have not alleged that they acted as affiants in support of the warrants or participated in their executions. *Defs.' Mot.* at 37. Plaintiffs respond that the USAO Defendants' role in facilitating the searches

was limited to administrative duties or other investigative functions not entitled to immunity. *Pls.' Opp'n* at 71-73. The Federal Defendants have the better argument.

Plaintiffs' response focuses on the USAO Defendants' role in using their authority to obtain purportedly unlawful search warrants as part of a "hoax criminal investigation" despite being aware that the applications "contained information known to be false and perjured." *Id.* at 71-72 (quoting *Second Am. Compl.* ¶¶ 18, 20). First, Plaintiffs' allegations of prosecutorial misconduct are wholly conclusory. Regarding the search warrants, they allege broadly that "[t]he search warrant order was issued under illegal and unlawful means in that the Federal defendants used the Legal Entity Enterprises' power to have the judiciary authorize the search and seizure warrants through the use of affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs' private business in violation [of] the United States criminal laws." *Second Am Compl.* ¶ 20. Aside from their general claims that every defendant was involved from the beginning in virtually every aspect of a conspiracy to defraud them despite knowing that Naicom was a legitimate business, Plaintiffs do not allege which of the USAO Defendants—U.S. Attorney Rodriguez-Velez, AUSA Capo-Iriarte, and AUSA Cannon—were involved in the preparation and submission of the search warrant application, or how they falsified it.

There is no suggestion of why the USAO Defendants would agree to lead a criminal conspiracy to defraud Plaintiffs or how they came together with the numerous other defendants to organize the conspiracy. The possibility that the

federal prosecutors believed that Naicom may have been engaged in illegal piracy presents an "obvious alternative explanation" for the USAO Defendants' conduct. *Iqbal*, 556 U.S. at 682. Moreover, even if the warrant applications contained false or perjured information, Plaintiffs do not allege that the USAO Defendants acted as affiants providing this information, and it would be equally plausible that the USAO Defendants were relying in good faith on bad information submitted by the private companies and/or FBI Defendants.[8]

Regardless, even if the Court were to find that Plaintiffs had sufficiently pleaded the USAO Defendants' involvement in submitting search warrant applications containing false information, the USAO Defendants would still be entitled to prosecutorial immunity. The *Buckley* Court outlined how absolute immunity attaches to actions taken in a prosecutor's role as an advocate, including "actions preliminary to the initiation of a prosecution and actions apart from the courtroom." 509 U.S. at 272 (quoting *Imbler*, 424 U.S. at 431 n.33). In doing so, it noted that "appearing before a judge and presenting evidence in support of a motion for a search warrant involved the prosecutor's 'role as advocate for the State,'" *id.* at 271 (quoting *Burns*, 500 U.S. at 491), and that "issuance of a search warrant is a judicial act . . . 'intimately associated with the judicial phase of the criminal process.'" *Id.* at 271 (quoting *Burns*, 500 U.S. at 492). The First Circuit has since further clarified that protected functions include:

[8] It is also not clear from the Second Amended Complaint how the USAO Defendants would have learned that the information in the affidavits was false. Merely alleging that the USAO Defendants had this knowledge due to their participation in the conspiracy, as Plaintiffs appear to have done, is conclusory.

> "appearing before a judge and presenting evidence in support of a motion for a search warrant," *Burns*, 500 U.S. at 491, and "prepar[ing] and filing ... [a criminal] information and [a] motion for an arrest warrant," *Kalina v. Fletcher*, 522 U.S. 118, 129 (1997). The basic "principle" of these cases is "that acts undertaken by a prosecutor in preparing for the initiation of judicial proceedings or for trial, and which occur in the course of his role as an advocate for the State, are entitled to the protections of absolute immunity." *Buckley*, 509 U.S. at 273.

Penate v. Kaczmarek, 928 F.3d 128, 136 (1st Cir. 2019) (alterations in original).

Plaintiffs have not alleged that the USAO Defendants falsified the affidavits themselves, served as supporting witnesses, or participated in the execution of the search warrants. Thus, even if Plaintiffs had properly pleaded that each USAO Defendant participated in the warrant application process, the USAO Defendants would still be entitled to absolute prosecutorial immunity for conduct undertaken in their roles as advocates. *See Omran v. United States*, No. 1:14-cv-00505-DBH, 2014 U.S. Dist. LEXIS 179017, at *15 (D.N.H. Dec. 30, 2014) ("[P]rosecutors are entitled to absolute immunity for their actions in procuring a warrant, so long as they do not act as attesting witnesses" (alteration in original) (quoting *Orth v. Balaam*, 528 F. App'x 723, 725-26 (9th Cir. 2013))); *Chan v. Cirilli*, No. 1:21-cv-11135-IT, 2022 U.S. Dist. LEXIS 211287, at *6 (D. Mass. Nov. 22, 2022) (prosecutors who allegedly fabricated criminal complaint affidavits and provided perjured testimony to grand jury were entitled to absolute immunity). This immunity necessitates the dismissal of all counts as pleaded against the USAO Defendants.

B. The Plaintiffs' RICO and RICO Conspiracy Claims

Plaintiffs' RICO claim falls short because their allegations rely too heavily on conclusory statements, and the conduct they allege does not establish a colorable

RICO claim. First, the allegations in the Second Amended Complaint are too threadbare to sufficiently plead the Federal Defendants' participation in a RICO enterprise and a pattern of racketeering activity. Second, even if the Court were to credit Plaintiffs' conclusory allegations, they nonetheless have failed to adequately plead predicate acts constituting a pattern of racketeering activity.

To state a civil RICO claim under 18 U.S.C. § 1962(c), a plaintiff must allege four elements: (1) conduct; (2) of an enterprise; (3) through a pattern; (4) of racketeering activity. *Lerner v. Colman*, 26 F.4th 71, 77 (1st Cir. 2022) (citing *Sedima, S.P.R.L. v. Imrex Co.*, 472 U.S. 479, 496 (1985)). "Racketeering activity" is defined to include a variety of predicate offenses, including, among other things, mail fraud, wire fraud, and theft of trade secrets. *Id.* § 1961(1). The civil-suit provision of the RICO statute grants the right to sue to "[a]ny person injured in his business or property by reason of a violation of" the substantive provisions of the statute. *Id.* § 1964(c).

Civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20 (1st Cir. 2000). "[I]n cases alleging civil RICO violations, particular care is required to balance the liberality of the Civil Rules with the necessity of preventing abusive or vexatious treatment of defendants." *Miranda v. Ponce Fed. Bank*, 948 F.2d 41, 44 (1st Cir. 1991), *abrogated on other grounds by Salinas v. United States*, 522 U.S. 52 (1997). "Civil RICO is an unusually potent weapon—the litigation equivalent

of a thermonuclear device. The very pendency of a RICO suit can be stigmatizing and its consummation can be costly." *Id.* Accordingly, "courts should strive to flush out frivolous RICO allegations at an early stage of the litigation." *Figueroa Ruiz v. Alegria*, 896 F.2d 645, 650 (1st Cir. 1990).

1. RICO Enterprise

a. Caselaw

In interpreting the RICO "enterprise" requirement, the Supreme Court has explained that "there is no restriction upon the associations embraced by the definition: an enterprise includes any union or group of individuals associated in fact." *Turkette*, 452 U.S. at 580. The enterprise concept is not unbounded, however, because an enterprise must be "an entity, for present purposes a group of persons associated together for a common purpose of engaging in a course of conduct." *Id.* at 583. In cases "involving an alleged associated-in-fact RICO enterprise, the existence of the charged enterprise does not follow, ipso facto, from evidence that those named as the enterprise's associates engaged in crimes that collectively may be characterized as a 'pattern of racketeering activity.'" *United States v. Cianci*, 378 F.3d 71, 81 (1st Cir. 2004).

Put differently, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of racketeering activity do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.* at 82. Ultimately, the First

Circuit has "read *Turkette* to impose a requirement that those associated in fact function as an ongoing unit and constitute an ongoing organization. Also important to such an enterprise is that its members share a common purpose." *Id.* at 82 (internal quotations omitted). Finally, the existence of an enterprise "is proved by evidence of an ongoing organization, formal or informal, and by evidence that the various associates function as a continuing unit." *Turkette*, 452 U.S. at 583.

b. Analysis

"Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice," *Iqbal*, 556 U.S. at 678, especially where "plaintiffs attempt to camouflage conclusory statements as allegations of fact." *A.G. ex rel. Maddox v. Elsevier, Inc.*, 732 F.3d 77, 81 (1st Cir. 2013). After sifting out Plaintiffs' conclusory statements, the RICO allegations as pleaded against the Federal Defendants are wafer thin, and the well-pleaded facts remaining are insufficient to establish that the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted).

The Second Amended Complaint pleads clearly and plausibly that the Federal Defendants investigated Plaintiffs for digital piracy, obtained and executed (on two occasions) search warrants for Plaintiffs' facilities, and coordinated with the DISH/NagraStar Defendants in the investigation, including permitting them to assist with the execution of the search warrants. Beyond these broad allegations, however, Plaintiffs' specific allegations are scant and conclusory. They assert that

the "investigation" was really a pretextual hoax concocted to steal their intellectual property. But the Second Amended Complaint is silent as to why or how at least ten employees of a U.S. Attorney's Office and the FBI—ranging from the U.S. Attorney herself to an FBI evidence technician and a computer scientist—came together to orchestrate and execute this scheme.

The Second Amended Complaint offers that, starting in 2017, all Defendants conspired at the outset and together "formed an Association In Fact, [including] Legal Entity Enterprises that would help the Association in Fact defendants advance the purpose and goals of the Racketeering Enterprises' conspiratorial objectives in misappropriating themselves from Plaintiffs' DISME intellectual technology property, and trade secrets and favor the Racketeering Enterprises' economic and market growth, at the expense of the Plaintiffs' financial and business detriment." *Second Am. Compl.* ¶¶ 17-18. It adds that the "Association-In-Fact defendants knowingly agreed, combined, and conspired to conduct the affairs of the Racketeering Enterprise in attempting and committing theft of trade secrets through a hoax criminal investigation operation." *Id.* ¶ 155.

Plaintiffs also assert that all DISH/NagraStar and Federal Defendants allegedly "supervised and approved" the set-top-box operation that involved a vast majority of the purported predicate acts. *Id.* ¶¶ 133-35. However, beyond pleading that each Federal Defendant and each DISH/NagraStar Defendant "supervised and approved" that operation, Plaintiffs do not elaborate on the role of any Federal Defendant, and instead assert that the operation involved the DISH/NagraStar

Defendants instructing the Toltec Defendants to purchase the set-top boxes for testing and provide one to the "Racketeering Enterprises." *Id.* ¶ 134.

These assertions are almost entirely vague, conclusory, and devoid of factual development that could explain how the alleged association in fact "function[ed] as an ongoing unit" or constituted an "ongoing organization." *Cianci*, 378 F.3d at 82 (internal quotations omitted). Aside from baldly asserting that each Federal Defendant individually agreed—for reasons unclear—to join the DISH/NagraStar conspiracy to steal Plaintiffs' property, Plaintiffs offer virtually no well-pleaded facts explaining how the conspirators functioned together as an ongoing unit or organization.

On that point, Plaintiffs offer only that "[t]he Association-In-Fact defendants had an ongoing organizational framework for carrying out the Racketeering Enterprises' criminal objectives. The Association-In-Fact defendants could not have carried out the intricate task of robbing Plaintiffs' Intellectual Property and Trade Secrets confidential information for the Racketeering Enterprises, unless it had some structure for making and communicating group decisions." *Second Am. Compl.* ¶ 130. The Court views this allegation as the epitome of a "[t]hreadbare recital[] of the elements of a cause of action, supported by mere conclusory statements." *Iqbal*, 556 U.S. at 678. It merely restates the requirement that the enterprise have an organizational framework, supported by nothing but the circular logic that the purported enterprise could not have succeeded unless it were truly an enterprise. There is, however, an obvious alternative explanation: that the information was

seized pursuant to a legitimate law enforcement investigation, not stolen as part of an elaborate conspiracy. These allegations do not adequately plead the existence of an "ongoing unit" or "ongoing organization" required for a RICO claim. *Cianci*, 378 F.3d at 82 (internal quotations omitted).

Furthermore, "criminal actors who jointly engage in criminal conduct that amounts to a pattern of racketeering activity do not automatically thereby constitute an association-in-fact RICO enterprise simply by virtue of having engaged in the joint conduct" and "[s]omething more must be found—something that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Id.*; *see also Bachman v. Bear Stearns & Co., Inc.*, 178 F.3d 930, 932 (7th Cir. 1999) (noting that a contrary rule would erroneously make "every conspiracy to commit fraud . . . a RICO [enterprise] and consequently every fraud that requires more than one person to commit . . . a RICO violation"). Plaintiffs allege that the Federal Defendants joined together with the other Defendants solely for the purpose of stealing Plaintiffs' "DISME intellectual technology property, and trade secrets," which they allegedly accomplished through executing the search warrants. *Second Am. Compl.* ¶¶ 18-21. While Plaintiffs assert that the DISH/NagraStar Defendants and DISH Corp. have been previously involved in trade secret misconduct, they do not allege that the Federal Defendants—or this association in fact as a whole—engaged or will engage in any misconduct unrelated to the one-off goal of stealing Plaintiffs' intellectual property. In its review of the Second Amended Complaint, the Court is unable to find the "[s]omething more" that

"must be found . . . that distinguishes RICO enterprises from ad hoc one-time criminal ventures." *Cianci*, 378 F.3d at 82.

As noted earlier, civil RICO claims "premised on mail or wire fraud must be particularly scrutinized because of the relative ease with which a plaintiff may mold a RICO pattern from allegations that, upon closer scrutiny, do not support it." *Efron*, 223 F.3d at 20. Ultimately, stripped of its conclusory allegations, the Court concludes that the Second Amended Complaint has not asserted sufficient facts to plead the Federal Defendants' involvement in a RICO enterprise, and Plaintiffs' RICO claim must fail.

2. Pattern of Racketeering Activity

Plaintiffs must also plead a "pattern of racketeering activity," which "means the commission of at least two related acts of racketeering activity during a period of ten years." *Humana, Inc. v. Biogen, Inc.*, 666 F. Supp. 3d 135, 147 n.4 (D. Mass. 2023) (citing 18 U.S.C. § 1961(5)). "Racketeering activity" is defined to include a variety of predicate offenses, including mail fraud, wire fraud, and theft of trade secrets. 18 U.S.C. § 1961(1). The First Circuit has observed that the Supreme Court has found "that the civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements." *In re Neurontin Mktg. & Sales Pracs. Litig.*, 712 F.3d 21, 34 (1st Cir. 2013) (citing *Holmes v. Secs. Investor Prot. Corp.,* 503 U.S. 258, 268 (1992)).

Plaintiffs allege that the purported RICO conspiracy's pattern of racketeering involved numerous predicate acts, including:

> [A]cts indictable under Mail Fraud (18 U.S.C. § 1341), Wire Fraud (18 U.S.C. § 1343), Conspiracy to Commit Mail And Wire Fraud (18 U.S.C. § 1341), Theft Of Trade Secrets Under The Defend Trade Secrets Act (18 U.S.C. § 1836 et seq.), while in addition, committing the possible underlying criminal offenses as prohibited under [the Computer] Fraud and Abuse Act (18 U.S.C. § 1030(a)); Stored Communications Act (18 U.S.C. §§ 2701-12); Digital Millennium Copyright Act (17 U.S.C. § 1201 et seq.), 18 U.S.C.A. § 2235-Search warrant procured maliciously; 18 U.S.C.A. § 1621- Perjury generally; 18 U.S.C.A. § 1001-Statements or entries generally, 18 U.S.C.A. § 912-Officer or employee of the United States; 18 U.S.C.A. § 2234-Authority exceeded in executing warrant; 18 U.S.C.A. § 2236-Searches without warrant, 18 U.S.C.A. § 1905-Disclosure of Confidential Information, while accomplishing their racketeering objectives.

Second Am. Compl. ¶ 132.

Most of these alleged offenses are not "predicate acts" under the RICO statute. Mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and theft of trade secrets (18 U.S.C. §§ 1831 and 1832)[9] qualify; the rest do not. *See* 18 U.S.C. § 1961(1) (listing qualifying offenses); *Pls.' Opp'n* at 13 ("The Federal defendants violated three predicate acts indictable under RICO: mail fraud; wire fraud; and misappropriation or theft of trade secrets"). The Court turns to the allegations concerning these three predicate acts.

a. Wire and Mail Fraud

"Mail or wire fraud requires proof of (1) a scheme to defraud based on false pretenses; (2) the defendant's knowing and willing participation in the scheme with the specific intent to defraud; and (3) the use of interstate mail or wire

[9] The statutory provision cited by Plaintiffs—18 U.S.C. § 1836—discusses civil proceedings for misappropriation of trade secrets and is not listed as a predicate act in 18 U.S.C. § 1961(1). Since the Court assumes Plaintiffs' reference to 18 U.S.C. § 1836 was in error, the Court has recharacterized their predicate-act allegations relating to theft of trade secrets as arising under 18 U.S.C. §§ 1831 and 1832.

communications in furtherance of the scheme." *Sanchez v. Triple-S Mgmt., Corp.*, 492 F.3d 1, 9-10 (1st Cir. 2007). "The 'in furtherance' requirement is to be read broadly." *United States v. Simon*, 12 F.4th 1, 33 (1st Cir. 2021). "[T]he mails need not be an essential element of the scheme. It is sufficient for the mailing to be incident to an essential part of the scheme, or a step in [the] plot." *Schmuck v. United States*, 489 U.S. 705, 710-11 (1989) (internal citations and quotations omitted).

Federal Rule of Civil Procedure 9(b) requires that "[i]n alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake." FED. R. CIV. P. 9(b); *see also Humana*, 666 F. Supp. 3d at 154 ("Civil RICO claims based on the predicates of mail or wire fraud must meet the heightened pleading standard of Rule 9(b)"). A complaint must specify "the time, place, and content of an alleged false representation." *United States ex rel. Kelly v. Novartis Pharms. Corp.*, 827 F.3d 5, 13 (1st Cir. 2016) (quoting *Doyle v. Hasbro, Inc.*, 103 F.3d 186, 194 (1st Cir. 1996)). Furthermore, "[t]he false or fraudulent representation [in a mail or wire fraud claim] must be material." *United States v. Appolon*, 715 F.3d 362, 367 (1st Cir. 2013) (first alteration in original) (citation omitted).

Plaintiffs' mail and wire fraud claims are limited to allegations that Mr. Jaczewski—in an operation "instructed" by Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel and "supervised and approved" by the Federal Defendants—used an alias to purchase two Naicom set-top boxes and a monthly subscription he maintained for two years. *Second Am. Compl.* ¶¶ 132-37. In Plaintiffs' view, each purchase or payment "constitutes a wire fraud racketeering act since [Mr. Jaczewski, acting

under the alias] Brian Parsons, posed as [a] legitimate client and used the interstate internet electronic services to access Naicom's website, and register online under the false pretenses of BRIAN PARSONS" and "made online payments through the use of interstate internet electronic services . . . to defraud and deprive Naicom Corporation of its legitimate products, intellectual property and trade secrets." *Id.* ¶ 134. Between the initial purchases and monthly subscription payments, Plaintiffs tally 22 acts of wire fraud. *Id.* ¶ 135. Finally, they also consider the initial purchase to constitute mail fraud because Mr. Jaczewski "posed as a legitimate client and used the United States Postal Services to have Naicom mail him the IPTV Set Top Box to a fake address." *Id.* ¶ 133.

Accepting these allegations as true, the Court concludes that the facts are insufficient to support Plaintiffs' wire and mail fraud claims because the purportedly fraudulent representations (limited to Mr. Jaczewski's use of an alias for the set-top-box purchase and subscription) were not material. Nor could the mail and wire fraud allegations be predicate acts for Plaintiffs' RICO claim because the set-top-box operation was not causally connected to Plaintiffs' damages.

A material statement "has a natural tendency to influence, or [is] capable of influencing, the decision of the decisionmaking body to which it was addressed" but plaintiffs "need not prove that the decisionmaker actually relied on the falsehood or that the falsehood led to actual damages." *Appolon*, 715 F.3d at 368 (alteration in original) (internal quotation omitted). In *Appolon*, the defendant provided untrue responses on a mortgage application, in response to questions "that specifically

sought information regarding the purchaser's income, assets, and intent to reside in the property." *Id.* The First Circuit considered the false responses material because the questions "were designed to assess the borrower's creditworthiness" and thus the statements "were capable of influencing [the lender's] decision." *Id.*

The purported false statements here are far afield from providing false financial information on a mortgage application. Naicom's set-top boxes are commercial electronic products sold in retail stores like Sam's Club, and its subscription services are available on Apple's AppStore as the Naicom TV App. *Second Am. Compl.* ¶ 70 ("On February 16, 2017, Apple Corporation approved Naicom Corporation App for Apple's AppStore as Naicom TV App"); *id.* ¶ 71 ("On December 15, 2017, Sam's Club approved Naicom Corporation to officially launch and distribute in their retail stores [] Naicom's IPTV Set Top Box which offered the distribution of tv programming to customers in Puerto Rico"). Parsing Plaintiffs' allegations, they allege that Mr. Jaczewski committed wire and mail fraud by providing a false name "of BRIAN PARSONS, fake Phone (727) 409-9464, fake Email: parsons.brian716@outlook.com and Address: 9079 FOURTH STREET NORTH SAINT PETERS FL 33702 IP: 70.127.233.139, and made online payments through the use of interstate internet electronic services using the PM Visa ending in 2775." *Id.* ¶ 134. Plaintiffs also allege Mr. Jaczewski used the alias of Brian Parsons when purchasing two Naicom set-top boxes. *Id.* ¶ 133.

The allegations confirm that Mr. Jaczewski used the false name of Brian Parsons. It is unclear, however, what Plaintiffs mean by a "fake Phone"—whether

Mr. Jaczewski used a different phone as part of the alias or if the number provided was entirely made up. Plaintiffs have not adequately pleaded that the remainder of the "false" statements are actually false. The Second Amended Complaint does not allege that email services require customers to use their real name in their email address. Thus, the Second Amended Complaint fails to allege that using an email with "parsons.brian" in the address is a false statement as there is no allegation that the address itself does not actually exist. It is unclear what Plaintiffs mean by a "fake" address, but again, the Second Amended Complaint also does not allege that online retail customers are prohibited from having a product shipped to any address they desire, and Plaintiffs have offered nothing to suggest that this constitutes a false representation.[10] Likewise, nothing in the Second Amended Complaint suggests that the IP address or credit card involved false statements.[11]

The Court is thus left to consider whether Mr. Jaczewski's purchase of two commercially available products and an accompanying subscription using the name Brian Parsons can support Plaintiffs' alleged mail and wire fraud violations. The Court concludes that it cannot, because—absent allegations to the contrary—a customer providing a false name in such circumstances does not have "a natural tendency to influence, [nor is it] capable of influencing, the decision of the

[10] In theory, Mr. Jaczewski could have provided an address that was entirely made up. This seems unlikely, however, in light of the Second Amended Complaint's allegations that the Defendants used the set-top boxes to attempt remote attacks on Naicom's servers. Had the boxes been shipped to an address that didn't exist, they would have been returned to Naicom as undeliverable, meaning that the Defendants could not have used them to launch sniffing attacks.

[11] To the contrary, in the Second Amended Complaint, Plaintiffs include a table listing all the payments made to Naicom by Mr. Jaczewski posing as Brian Parsons. *Second Am. Compl.* ¶ 136. In the Court's view, these payments confirm that the credit card number provided by Mr. Jaczewski was valid.

decisionmaking body to which it was addressed." *Appolon*, 715 F.3d at 368. Nothing in the Second Amended Complaint suggests that the use of this alias was material to Plaintiffs' decision to sell Mr. Jaczewski their commercially available product. There is no allegation that Mr. Jaczewski was either known to Plaintiffs or prohibited from purchasing Plaintiffs' products. What is missing is an allegation that the alias could have reasonably affected the "decision of the decisionmaking body" (for example, Naicom's sales department) to process Mr. Jaczewski's payment or ship his order. Absent allegations regarding how Mr. Jaczewski's alias affected Naicom's decision to sell him their product, Plaintiffs have not pleaded material fraud with the requisite particularity. Plaintiffs' wire and mail fraud claims cannot stand and thus do not count as predicate acts in support of their RICO claim.

Furthermore, even if the Court did find the alleged representations material, Plaintiffs' claims fall short of the causation standard required for a wire or mail fraud-based RICO claim. *Neurontin*, 712 F.3d at 34 ("[T]he civil RICO provision's 'by reason of' language contains both but-for causation and proximate causation requirements" (citing *Holmes,* 503 U.S. at 268)). "The 'central question' in evaluating proximate causation in the RICO context 'is whether the alleged violation led directly to the plaintiff's injuries.'" *Sterling Suffolk Racecourse, LLC v. Wynn Resorts, Ltd.*, 990 F.3d 31, 35 (1st Cir. 2021) (quoting *Anza v. Ideal Steel Supply Corp.*, 547 U.S. 451, 461 (2006)). Quoting the U.S. Supreme Court, the First Circuit has noted that "[a] link [between the RICO predicate acts and plaintiff's injuries] that is too remote, purely contingent, or indirect is insufficient to show proximate cause." *Id.* (alterations in

original) (quoting *Hemi Grp., LLC v. City of New York*, 559 U.S. 1, 9 (2010)). In addition, the First Circuit has identified "three functional factors with which to assess whether proximate cause exists under RICO."[12] *Id.* (quoting *Neurontin*, 712 F.3d at 35-36)). The but-for causation question, in contrast, asks whether, absent the defendant's violation, the plaintiff would have suffered the same injury. *See Neurontin*, 712 F.3d at 34.

Here, the alleged violations fail both causation tests because Plaintiffs portray the set-top-box operation as an unmitigated failure that only provided further proof that Naicom was a legitimate company. They allege that "after testing Naicom TV several times to identify if it was providing DISH programming, on each case the test *revealed no DISH content*." *Second Am. Compl.* ¶ 90 (emphasis added). After attempting to use the boxes to penetrate Plaintiffs' network and steal their secrets, the "Dish/Nagrastar defendants also informed the Racketeering Enterprises that the Association in Fact defendants couldn't penetrate Naicom's Data Center computers, servers, encoders electronic security system, and that a physical intrusion was necessary to extract the intellectual property from the computers, servers, and encoders by physical access." *Id.* ¶ 93. They allege further that the operation did not yield evidence that would support a search warrant and thus the defendants had to

---

[12] These factors are:

> (1) "concerns about proof" because "the less direct an injury is, the more difficult it becomes to ascertain the amount of a plaintiff's damages attributable to the violation, as distinct from other, independent, factors," . . . (2) "concerns about administrability and the avoidance of multiple recoveries," . . . and (3) "the societal interest in deterring illegal conduct and whether that interest would be served in a particular case[.]"

Sterling Suffolk Racecourse, 990 F.3d at 35-36 (quoting *Neurontin*, 712 F.3d at 35-36).

provide "affidavits they knew contained material information known to be false and perjured to create probable cause to gain legal access into Plaintiffs[']s private business." *Id.* ¶ 20.

As the Court understands the Second Amended Complaint, Plaintiffs allege that the Defendants conspired from the outset to steal their intellectual property. The set-top-box operation was an attempt to steal Plaintiffs' secrets by reverse engineering the technology and/or penetrating Plaintiffs' networks. But the operation failed. All the Defendants gained was more proof that Naicom was a legitimate company, and they then had to resort to falsifying affidavits to justify physical access to Naicom's Data Center (through search warrants) that would finally allow them access to the desired technology. Plaintiffs have not alleged any harm prior or unrelated to the execution of the warrants. Nor have Plaintiffs alleged that Defendants would not have sought and executed the search warrants had they not undertaken the set-top-box operation.

The Court concludes that there is no connection—proximate or but-for—between the allegedly fraudulent set-top-box purchase and the Defendants acquiring Plaintiffs' intellectual property during the execution of the warrants. The alleged mail and wire fraud is "too remote" from Plaintiffs' alleged harms, *Hemi Grp.*, 559 U.S. at 9, and there is no indication that Plaintiffs would not have suffered their alleged harms absent the set-top-box operation. Plaintiffs' Second Amended Complaint thus falls short on both the materiality and causation standards for wire and mail fraud as predicate acts.

b. Theft of Trade Secrets

Plaintiffs also plead that the Federal Defendants committed RICO predicate acts by misappropriating their trade secrets. *See Second Am. Compl.* ¶¶ 138-41; *Pls.' Opp'n* at 13 ("The Federal defendants violated three predicate acts indictable under RICO: mail fraud; wire fraud; and misappropriation or theft of trade secrets"). As noted above, RICO predicate offenses include any act indictable under 18 U.S.C. § 1832, relating to theft of trade secrets under the DTSA. 18 U.S.C. § 1961(1). 18 U.S.C. § 1832 provides that "[w]hoever, with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information," or attempts to do so, shall be subject to criminal penalties. *Id.* § 1832(a)(1), (a)(4). "Trade secret" is defined broadly to include "all forms and types of financial, business, scientific, technical, economic, or engineering information," as long as "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information." *Id.* § 1839(3). Critically, however, the DTSA also provides that "[t]his chapter does not prohibit . . . any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1).

The scope of Plaintiffs' DTSA theories is unclear. They allege clearly that the Federal Defendants violated the DTSA on August 27 and 29, 2019 (the dates of the searches) by "facilitating and assisting" the DISH/NagraStar Defendants' entry into Naicom's facility to steal Naicom's trade secrets. *Second Am. Compl.* ¶ 141. Their other theories are far more ambiguous, alleging generally that "[b]eginning on or before August 7, 2017," Mr. Gedeon, Mr. Smith, Mr. Eichhorn, and Ms. Rinkel, along with the Federal Defendants: "stole, and without authorization misappropriated, took, carried away, or by fraud, artifice, or deception obtained trade secrets," *id.* ¶ 138; "did without authorization, spy, reverse engineered, copied, duplicated, downloaded, uploaded, altered, destroyed, replicated, transmitted, delivered, sent, communicated, and/or conveyed intellectual property and trade secrets," *id.* ¶ 139; and "misappropriated, obtained, or converted without authorization [the trade secrets] to the economic benefit of [the] Racketeering Enterprises and other defendant coconspirators." *Id.* ¶ 140. This section of the Second Amended Complaint, however, offers no additional details as to when or how any specific Federal Defendant violated the DTSA.

The only clarity in Plaintiffs' 75-page opposition is their contention that "[t]he record . . . supports the finding that the Dish/Nagrastar defendants' misapprop[riation of] Plaintiffs' trade secrets by illegal means is unlawful, given the way [the] Dish/Nagrastar defendants obtained the same through the illegal search warrant, warrantless executions, and trespass, orchestrated and facilitated by the Federal defendants." *Pls.' Opp'n* at 66. Based on the content of Plaintiffs' Second

Amended Complaint and their statements in opposition to the Federal Defendants' motion to dismiss, the Court narrows the scope of the DTSA inquiry to the Federal Defendants' actions related to obtaining and executing the search warrants—discarding any other DTSA allegations as pleaded with insufficient particularity against any Federal Defendant.[13]

The Federal Defendants argue that Plaintiffs' misappropriation of trade secrets claims should be dismissed because "the plaintiffs have not adequately alleged the existence of any trade secrets" and because "Congress specifically exempted from the statute's criminal and civil provisions 'any otherwise lawful activity conducted by a governmental entity of the United States.'" *Defs.' Mot.* at 32-33 (quoting 18 U.S.C. § 1833(a)(1)). The Court concludes that Plaintiffs have not adequately impugned the validity of the warrants and the Federal Defendants' conduct is thus exempt from DTSA liability as authorized law enforcement activity.

The Federal Defendants submit that "the plaintiffs here acknowledge that the government obtained and searched under the authority of a warrant," which "makes the Federal Defendants' actions here presumptively lawful." *Id.* at 33. They add that the Supreme Court has observed that "[t]he fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith.'" *Id.* at 23 (quoting *Messerschmidt v. Millender*, 565 U.S. 535, 546 (2012)). The Federal Defendants

[13] Regardless, most of these allegations appear to be incorporated in the allegations related to the search warrants. For example, it is unclear what Plaintiffs are referring to in alleging that the Federal Defendants "copied, duplicated, [and] downloaded" their confidential information aside from the allegations relating to the search warrant execution. *Second Am. Compl.* ¶ 139.

assert further that "[t]he plaintiffs' conclusory allegations that the warrant was 'unlawful,' or secured using an affidavit in support of probable cause containing 'material information known to be false and perjured' are insufficient to [impugn the presumptive validity of the warrant]." *Id.* at 33 (citations omitted).

Plaintiffs respond that "the procurement of the issuance and execution of the search and seizure warrant and the subsequent warrantless search and seizure execution were illegal and unconstitutional." *Pls.' Opp'n* at 30. Because Plaintiffs dispute the validity of the warrants, the Court addresses this issue first.

The parties agree that the relevant standard for evaluating the validity of a warrant is the *Franks v. Delaware* framework, which requires Plaintiffs to adequately allege that both (1) "a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit" and (2) "the allegedly false statement is necessary to the finding of probable cause." *United States v. Reiner*, 500 F.3d 10, 14 (1st Cir. 2007) (quoting *Franks v. Delaware,* 438 U.S. 154, 155-56 (1978)). Plaintiffs cite ten statements that they allege Defendants "falsely submitted to the Court." *Id.* at 31. The Court has examined each and concludes that none supports Plaintiffs' claims.

Plaintiffs' first purportedly false statement is the Federal Defendants' statement that they believed there was probable cause that Plaintiffs violated copyright and money laundering laws. *Id.* Plaintiffs allege that this statement is false because:

> The execution of the search and seizure warrant in this case did not produce any criminal evidence whatsoever; there was no probable cause.

> That is why the United States never opposed Plaintiffs' Motion for Return of Property under Rule 41(g) of the Fed.R.Crim.P. In fact, they didn't even contend the serious violations Plaintiffs imputed under *Franks* in the Rule 41(g) motion.

Id. This logic is unavailing. Plaintiffs cannot rely on the circular reasoning that the search's alleged failure to produce incriminating evidence thereby proves that the Defendants could not have believed there was probable cause to search. *See Karamanoglu v. Town of Yarmouth*, 15 F.4th 82, 88 (1st Cir. 2021) (defining the probable cause inquiry as "whether, on balance, the facts *known to the officer at the time of the arrest* support probable cause").

Equally inadequate is Plaintiffs' claim that the Federal Defendants' failure to oppose Plaintiffs' motion to return the seized property proves not only that the seized property was not incriminating, but also that there was no probable cause to search in the first place. *See United States v. Pierre*, 484 F.3d 75, 87 (1st Cir. 2007) ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return"). The government's return of the seized hard drives and thumb drives, which—unlike drugs or illegal firearms—are not inherently contraband and can easily be downloaded or duplicated, is consistent with *Pierre*.

Furthermore, Plaintiffs are simply incorrect that success on a Rule 41(g) motion conclusively establishes the invalidity of a search. Rule 41(g) allows motions for return of property from "[a] person aggrieved by an unlawful search and seizure of property *or* by the deprivation of property." FED. R. CRIM. P. 41(g) (emphasis supplied). Without more, the property's return alone cannot demonstrate an absence of probable cause to search and seize in the first place. Ultimately, Plaintiffs' first

purportedly false statement offers nothing to undermine the validity of the warrants and searches.

Second, Plaintiffs offer that the Federal Defendants "assured the Court they had evidence based on an investigation conducted by Nagrastar of Naicom's unauthorized use of Direct TV signal to distribute its programing to its paid subscribers." *Pls.' Opp'n* at 32. Plaintiffs assert that this statement was false because "[t]he United States did not produce any evidence as to the above allegations . . . [i]n contrast, Naicom did produce all the documentary evidence establishing that they were authorized to distribute the copyright material." *Id.*

Again, Plaintiffs appear to be suggesting that exculpatory evidence they produced during the search proves that the affidavit was false. These conclusory assertions tied together by circular logic do not adequately demonstrate the falsity of the affidavit. While Plaintiffs contend that the affidavit did not "produce any evidence" supporting the suggestion that Naicom was distributing DirecTV content without authorization, the affidavit avers that Naicom's system displayed DirecTV error messages on at least 16 channels (and includes a photo of the message), that Naicom's satellite dishes were precisely oriented in a manner necessary to receive DirecTV satellite signals, that representatives of the companies offering some channels Naicom purported to provide confirmed that Naicom was not licensed to provide them, and other indicia of piracy. *See Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1 at 272-94, *Aff. in Supp. of an Application for a Search Warrant* (*Warrant*

Aff.). Simply put, Plaintiffs' argument that the affidavit contained no evidence of piracy is incorrect.

Third, Plaintiffs assert that, during a 2018 FBI site visit of Naicom's property, Mr. Vega "repeatedly told the agent that Naicom was a legal corporation and showed the agent a certificate from the National Cable Television Cooperative (NCTC) on the wall," yet the Federal Defendants still "filed the affidavit containing materially false and perjured statements." *Pls.' Opp'n* at 32. It is not clear specifically which "materially false and perjured statements" Plaintiffs are referring to, but the affidavit states that the FBI called NCTC's management group, which confirmed that Naicom was *not* a member. *Warrant Aff.* ¶ 15. Nothing in Plaintiffs' assertion that Mr. Vega told the FBI his company was legitimate and showed them a certificate on the wall establishes that the affidavit's claim—that NCTC management represented to the FBI that Naicom was not a member—was perjured.

Fourth, Plaintiffs contend that the affidavit's claim that Naicom was using the NCTC certificate to create the appearance of legal access to channels was "a false and perjured statement" because an FBI agent took pictures of "Naicom's National Rural Telecommunications Cooperative 'NRCT' Certificate" and Naicom had licenses with other networks. *Pls.' Opp'n* at 32-33.

Fifth, Plaintiffs focus on the affidavit's claim that FBI agents spoke with NCTC management, who confirmed that Naicom was not a member of their organization. *Id.* at 33. They allege that this "is a false and perjured statement" because Naicom provided evidence that it is a member of the NRTC. *Id.*

The distinction between NCTC and NRTC here is somewhat confusing. It appears Plaintiffs are alleging that the FBI took pictures of a NRTC certificate on the wall but incorrectly referred to it in the affidavit as a NCTC certificate, or that the FBI mistook their NRTC certificate for an NCTC certificate. However, Plaintiffs also claim that the affidavit's assertion that they are not a member of the NCTC is a perjured statement because they provided evidence that they are a member of the NRTC. Plaintiffs offer no evidence that the latter statement was perjured because proving they are a NRTC member does not contradict the claim that they are not a NCTC member. To the extent that the FBI may have misidentified a NRTC certificate as a NCTC certificate, the record does not suggest that this "allegedly false statement is necessary to the finding of probable cause," especially given the strength of the other supporting claims in the affidavit. *United States v. Patterson*, 877 F.3d 419, 424 (1st Cir. 2017) (quoting *Franks*, 438 U.S. at 156).

Sixth, Plaintiffs turn to the affidavit's assertion that FBI agents contacted officials at HBO and DirecTV, who verified that Naicom did not have a relationship with their organizations despite offering HBO content. *Pls.' Opp'n* at 33. Plaintiffs claim that "[t]his is a false and perjured statement" because "Naicom provided evidence that it is licensed to distribute HBO and Cinemax programming." *Id.* (citing *Pls.' Opp'n to DISH/NagraStar Mot.*, Attach. 1 at 356 (HBO invoice dated August 31, 2019, for roughly $200 per month for "Cable – Private Home" services). Plaintiffs' claim is unpersuasive for two reasons: (1) this invoice for inexpensive "Cable – Private Home" services does not appear to provide evidence of a licensing agreement; and (2)

Plaintiffs have not directly contradicted the purportedly perjured claim, which was that HBO and DirecTV officials represented to the FBI that they did not have a relationship with Naicom.

Seventh, Plaintiffs focus on the affidavit's claim that the "external appearance of the Data Center offered indicia of piracy," calling it a "false and perjured statement" because "[a]t the conclusion of the search and seizure warrant execution the FBI agents found that [] Naicom's equipment (encoders) were provided by the networks authorizing the programming distribution and that the use of the satellite was in fact to download the codes provided by the networks." *Id.* at 33-34. Plaintiffs again rely on circular logic, as the discovery of exculpatory evidence at the conclusion of a warrant's execution does not provide a "substantial preliminary showing" that the underlying affidavit was perjured. *Franks*, 438 U.S. at 155-56.

Plaintiffs' eighth point suffers from the same defect. They claim that the affidavit's statements that there were suspicious financial transactions between Naicom and other businesses owned by Mr. Quinones and Mr. Vega were false and perjured because "[d]uring the execution of the Search Warrant S/A Lange interviewed employees from the Business Office and was provided with financial records" which established "that none of the Corporations were involved in any money laundering activities." *Pls.' Opp'n* at 34. Again, the fact that a search did not uncover incriminating evidence does not establish that it was predicated on a perjured affidavit.

Plaintiffs' ninth point takes issue with the affidavit's request to seize computers and data based on claimed probable cause that they contained evidence. *Id.* at 34-35. Plaintiffs contend that this statement was perjured because the "FBI agents were not looking for any criminal evidence" during the search and they did "not find[] any evidence whatsoever of the crimes described in the warrant, which also denied any probable cause." *Id.* at 34. The Court does not fully follow Plaintiffs' logic across these seemingly contradictory assertions, but they appear to utilize the same circular reasoning (the assertion of probable cause was perjured because the resulting search "denied any probable cause"), along with the conclusory contention that the FBI was not actually looking for evidence.[14] These claims do not undermine the validity of the warrants.

Tenth, Plaintiffs claim that the affidavit's request to seize evidence relating to statutory violations was "false and perjured" because the FBI did not find any evidence at the conclusion of the search. *Id.* at 35. Beyond the fact that this argument relies on the same circular logic, an affidavit's request to seize "things and . . . records" is not an assertion of fact and cannot be false or perjured. *Id.*

To summarize, none of these purportedly false statements, alone or in combination, satisfies Plaintiffs' burden under the *Franks* standard to overcome the presumed validity of the warrants. Moreover, Plaintiffs offer several additional arguments that are similarly unavailing.

[14] Apart from their general contention that the investigation was a hoax invented to steal their intellectual property, Plaintiffs have provided no support for this latter assertion. As noted above, it is equally plausible—if not more so—that the FBI was looking for evidence as part of a legitimate criminal investigation.

Plaintiffs submit that the August 29, 2019 search was "illegal" and "warrantless" because "[t]he Federal and Dish/Nagrastar defendants knew for a fact that the first search warrant execution had already denied any criminal wrongdoing, and that the initial alleged probable cause had dissipated." *Id.* at 42. This assertion—that the Federal Defendants knew probable cause had dissipated—is wholly conclusory (especially in light of Plaintiffs' argument that the entire investigation was a hoax, and the agents knew probable cause never existed). Furthermore, the warrants did not expire until September 4, 2019 and courts generally recognize a "reasonable continuantion rule" providing that a search may be reasonably continued if the warrant remains valid.[15] *See United States v. Keszthelyi*, 308 F.3d 557, 568-69 (6th Cir. 2002) (describing the rule and collecting cases). Plaintiffs have not offered any well-pleaded, nonconclusory allegations suggesting that the continuance here was unreasonable.[16]

Plaintiffs also contend that the searches were unlawful because the Federal Defendants did not follow the procedure to obtain a Stored Communications Act warrant (also known as a disclosure order or a SCA order). *Pls.' Opp'n* at 37-38.

---

[15] The "reasonable continuation rule" requires the satisfaction of two conditions: 1) "the subsequent entry must indeed be a continuation of the original search, and not a new and separate search"; and 2) "the decision to conduct a second entry to continue the search must be reasonable under the totality of the circumstances." *Keszthelyi*, 308 F.3d at 569.

[16] The closest Plaintiffs come to a nonconclusory allegation is their assertion that U.S. Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned, after the execution of the first search warrant, that Naicom complied with "all the programming distribution contract and agreements." *Second Am. Compl.* ¶ 103. But this allegation is still conclusory, and it is undercut by the sentence immediately following it, which alleges that the USAO Defendants instructed S/A Pearson "to order Darwin Quinones and Victor Vega to report to the FBI Offices in San Juan with the licensing contracts for an interview regarding Naicom's company." *Id.* Clearly, whatever U.S Attorney Rodriguez-Velez and Assistant U.S. Attorney Capo-Iriarte learned did not absolve Naicom of wrongdoing; otherwise, there would have been no need to conduct an interview.

However, as the Federal Defendants observe, "the government appropriately opted for a traditional search warrant in this case because it sought to seize evidence of the plaintiffs' piracy operation rather than to require the plaintiffs to disclose certain electronic communications." *Defs.' Reply* at 18.

While SCA warrants and traditional search warrants are not the same thing, the Court has no trouble concluding that the Federal Defendants' decision to proceed via search warrant was proper. As one court has explained:

> SCA warrants "are not like the search warrants used in the physical world: they are 'executed' when a law enforcement agent delivers (sometimes by fax) the warrant to the [service provider]. The [service provider], not the agent, performs the 'search'; the [service provider] 'produces' the relevant material to the agent; the user associated with the inbox often never learns that his inbox has been 'searched.' In sum, these are not search warrants at all and to call them such confuses legal terminology."

In re Info. Associated with @gmail.com, No. 16-mj-00757 (BAH), 2017 U.S. Dist. LEXIS 130153, at *52-53 (D.D.C. July 31, 2017) (quoting Paul K. Ohm, *Parallel–Effect Statutes and E–Mail "Warrants": Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610-11 (2004)). Additionally, the standard for an SCA order is "less stringent than the probable cause standard generally required for a search warrant." *United States v. Taylor*, 54 F.4th 795, 804 (4th Cir. 2022). Finally, even if the Federal Defendants were seeking information protected by the SCA, the statute gives them the option of seeking either an SCA order or a traditional search warrant.[17] *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for

[17] Further, "the statute offers no express direction as to when the government should seek a warrant versus" a SCA order." *Taylor*, 54 F.4th at 804.

such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same).

Plaintiffs' argument is groundless because the Federal Defendants were primarily—if not entirely—seeking information not protected by the SCA. Regardless, they obtained a search warrant for the facility and computer systems, thereby satisfying the requirements of the SCA.

Plaintiffs also argue again that "the Federal defendants cannot raise at this stage a legal defense which the Federal defendants abandoned when they did not oppose the Motion for Return of Property under Rule 41(g) proceedings." *Pls.' Opp'n* at 43. However, as the Court has already explained, the government's decision not to oppose a motion to return property does not affect the validity of the warrants or seizure. *See Pierre*, 484 F.3d at 87 ("Once seized property is no longer needed as evidence, a criminal defendant is presumed to have the right to its return").

Finally, while Plaintiffs contend that permitting the DISH/NagraStar Defendants to assist with the search was unlawful, they acknowledge that "Congress has explicitly authorized the practice." *Pls.' Opp'n* at 39 (citing 18 U.S.C. § 3105). Further, although they contend that any civilian assisting with a search "must have been serving a legitimate investigative function," *id.*, Plaintiffs fail to make any well-pleaded, nonconclusory allegation that the DISH/NagraStar Defendants were not serving such a function. Indeed, Plaintiffs do not offer any persuasive argument that

would permit the Court to find that the DISH/NagraStar Defendants' presence rendered the search illegal.[18]

In sum, Plaintiffs have failed to adequately challenge the validity of the search warrants or to establish that any Federal Defendant exceeded the bounds of his or her lawful authority. Plaintiffs have thus failed to plead a DTSA violation as a predicate act in support of their RICO claim. *See* 18 U.S.C. § 1833(a)(1) ("This chapter does not prohibit . . . any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"). Absent both an enterprise and a pattern of racketeering activity, Plaintiffs' RICO (Count I) claim must be dismissed as to the Federal Defendants.

These same pleading shortfalls doom Plaintiffs' RICO conspiracy claim as to the Federal Defendants. *See Efron*, 223 F.3d at 21 ("A conspiracy claim under section 1962(d) may survive a *factfinder's* conclusion that there is insufficient evidence to prove a RICO violation, but if the pleadings do not state a substantive RICO claim upon which relief may be granted, then the conspiracy claim also fails" (citations omitted) (emphasis in original)); *see also Salinas v. United States*, 522 U.S. 52, 64 (1997) ("A conspirator must intend to further an endeavor which, if completed, *would satisfy all of the elements of a substantive criminal offense*, but it suffices that he adopt

[18] Plaintiffs quote *Bellville v. Town of Northboro*, 375 F.3d 25 (1st Cir. 2004), for the proposition that "it might be a better practice, if circumstances permit, for law enforcement officers to disclose to the magistrate that civilians will be involved in the execution of the search and for the warrant to indicate that the magistrate permitted this involvement." *Pls.' Opp'n* at 40 (footnotes omitted) (quoting *Bellville*, 375 F.3d at 33-34). They fail to quote the preceding sentence, which states, "we will not improvise a rule that seems unnecessary in light of the overarching requirement that the use of civilians in the execution of a search must still meet the constitutional standard of reasonableness." *Bellville*, 375 F.3d at 33. The Court declines to accept Plaintiffs' invitation to convert the best practice outlined by the First Circuit into a rule.

the goal of furthering or facilitating the criminal endeavor" (emphasis supplied)). As such, the Court also dismisses Plaintiffs' RICO conspiracy claim (Count II) as to the Federal Defendants.

C. Plaintiffs' DTSA, CFAA, SCA, and DMCA Claims

The Court's determination that the Federal Defendants' conduct during the execution of the search warrants did not exceed the bounds of a lawful warrant is ultimately also fatal to Plaintiffs' DTSA, CFAA, SCA, and DMCA claims, because each statute has a similar exemption for law enforcement activity.

1. The DTSA Claim

Plaintiffs' freestanding DTSA claim alleges the same violation as the DTSA claims offered as predicate acts for the RICO claim, and thus fails for the reasons previously described. While the DTSA does provide a private right of action for owners "of a trade secret that is misappropriated . . . if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce," 18 U.S.C. § 1836, this right of action cannot be used to challenge "otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State." *Id.* § 1833(a)(1). The Court dismisses Plaintiffs' DTSA claim (Count VI) as to the Federal Defendants.

2. The CFAA Claim

The CFAA contains virtually the same exception for law enforcement activity. *Compare* 18 U.S.C. § 1833(a)(1) (the DTSA "does not prohibit or create a private right of action for any otherwise lawful activity conducted by a governmental entity of the United States, a State, or a political subdivision of a State"), *with id.* § 1030(f) (the

CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States"). In *Smith v. Aldridge*, the plaintiff "allege[d] that Defendant stole his smartphone, which is legally protected under CFAA" but also admitted "that Defendant had a warrant when she accessed his phone." No. 3:17-cv-01485-HZ, 2018 U.S. Dist. LEXIS 47021, at *18 (D. Or. Mar. 22, 2018). The district judge observed that "Defendant, therefore, had legal authority to access Plaintiff's phone at the time that she did" and because "Plaintiff admits that Defendant had a warrant, Plaintiff would have to show that the warrant was invalid in order to show that the access was unauthorized . . .. [For the plaintiff] to prevail on this CFAA claim, the Court would have to determine that Plaintiff's Fourth Amendment Rights were violated." *Id.* at *18 & n.4.

Because the Federal Defendants' challenged conduct was "lawfully authorized investigative . . . activity" under the search warrants, Plaintiffs have not pleaded a viable CFAA claim.

3. The SCA Claim

Turning to the SCA claim, "courts in the First Circuit have consistently applied CFAA caselaw in analyzing the SCA. . . . Thus, the Court's analysis under this statute is the same as under the CFAA." *Sun West Mortg. Co. v. Flores*, No. 15-1082 (GAG), 2016 U.S. Dist. LEXIS 31149, at *11 (D.P.R. Mar. 10, 2016) (citation omitted); *see also Cheng v. Romo*, No. 11-10007-DJC, 2012 U.S. Dist. LEXIS 169535, at *10 (D. Mass. Nov. 28, 2012) ("Other district courts within this Circuit have addressed 'access without authorization' and 'exceeding authorization' in considering the analogous

provision of the CFAA"). As the Court noted previously, even if the Federal Defendants were seeking information protected by the SCA, the statute gives them an option of seeking either an SCA order or a traditional search warrant. *See* 18 U.S.C. § 2703(b) (the government may obtain "a court order for such disclosure under subsection (d) of this section" *or* "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure"); *id.* § 2703(c) (same). Furthermore, even if the warrants were not valid, the SCA still provides that "[a] good faith reliance on . . . a court warrant or order . . . is a complete defense to any civil or criminal action brought under this chapter or any other law." *Id.* § 2707(e).

Even if the Court were to assume that the Federal Defendants seized electronic communications protected by the SCA, they did so pursuant to valid warrants and thus did not violate the statute. Furthermore, even if the warrants were not valid, Plaintiffs' allegations of bad faith by the Federal Defendants are conclusory and the Federal Defendants would thus still be protected by the good faith defense. *See John K. MacIver Inst. for Pub. Pol'y, Inc. v. Schmitz*, 243 F. Supp. 3d 1028, 1035 (W.D. Wis. 2017), *aff'd*, 885 F.3d 1004 (7th Cir. 2018) ("Given the absence of any case law even suggesting that a state search warrant issued under similar circumstances may be invalid under the SCA, plaintiff's conclusory allegation of a lack of good faith is also wholly insufficient to support a claim that defendants 'actually knew that the [warrant] was invalid [under the SCA]'" (emphasis omitted) (alterations in original) (quoting *Sams v. Yahoo! Inc.*, 713 F.3d 1175, 1181 (9th Cir, 2013))). Plaintiffs' SCA

claim will not lie against the Federal Defendants for essentially the same reasons as their CFAA claim.

4. The DMCA Claim

Similarly, the DMCA explicitly provides that it "does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e). This language is virtually identical to the CFAA's law enforcement exception. *Cf.* 18 U.S.C. § 1030(f) (the CFAA "does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State"). This provision of the DMCA has been interpreted as "broadly exempting official law enforcement activity." *Green v. U.S. Dep't of Just.*, 392 F. Supp. 3d 68, 77 (D.D.C. 2019).

As with the DTSA, CFAA, and SCA claims, even assuming Plaintiffs had established all the other elements of a DMCA claim, their claim would still be stymied by the statute's law enforcement exception. Plaintiffs' DTSA, CFAA, SCA, and DMCA claims all fail as pleaded against the Federal Defendants because the challenged searches were conducted pursuant to lawfully authorized warrants.

D. The Plaintiffs' PTSA Claim

The Federal Defendants contend that Plaintiffs' Puerto Rico Uniform Trade Secrets Act claim is barred by the Westfall Act. *Defs.' Mot.* at 35-36. The Court agrees.

"Under the Westfall Act, the Attorney General can certify that a federal employee named as a defendant in a civil case was 'acting within the scope of his office or employment at the time of the incident' that serves as the basis for a tort claim against that employee." *Lyons v. Brown*, 158 F.3d 605, 606 (1st Cir. 1998) (quoting 28 U.S.C. § 2679(d)(1)). The Act provides that "[u]pon certification . . . any civil action or proceeding commenced upon such claim in a United States district court shall be deemed an action against the United States . . . and the United States shall be substituted as the party defendant." *Vélez-Díaz v. Vega-Irizarry*, 421 F.3d 71, 75 (1st Cir. 2005) (alterations in original) (quoting 28 U.S.C. § 2679(d)(1)). While certification is sufficient to substitute the United States as defendant and dismiss the federal employees from the case, the certification is "provisional and subject to judicial review." *Davric Me. Corp. v. U.S. Postal Serv.*, 238 F.3d 58, 65 (1st Cir. 2001) (citing *Gutiérrez de Martínez v. Lamagno*, 515 U.S. 417, 434 (1995)). If plaintiffs are able to show that the employees acted outside the scope of their employment, the employees may be re-substituted as the party defendants. *Davric*, 238 F.3d at 65; *Aversa v. United States*, 99 F.3d 1200, 1208 (1st Cir. 1996).

The Federal Defendants submit that Plaintiffs' PTSA claim "is barred because Congress provided in the Westfall Act that the exclusive remedy for claims for negligent or wrongful acts or omissions of federal employees acting in the scope of office or employment is a suit against the United States under the Federal Tort Claims Act" and "the Attorney General's designee has certified scope of office or employment" for the Federal Defendants. *Defs.' Mot.* at 35-36. This is sufficient to

substitute the United States as a defendant: "Upon certification . . . any civil action or proceeding . . . *shall* be deemed an action against the United States . . . and the United States *shall* be substituted as the party defendant." 28 U.S.C. § 2679(d)(1) (emphasis supplied).

The Federal Defendants argue further that once the United States has been substituted, the PTSA claim "must be dismissed as to the government as well" because "'[u]pon certification, any action or proceeding subject to' the Act 'shall proceed in the same manner as any action against the United States filed pursuant to' the FTCA 'and shall be subject to the limitations and exceptions applicable to those actions.'" *Defs.' Mot.* at 36 (quoting 28 U.S.C. § 2679(d)(4)). According to the Federal Defendants, Plaintiffs have not complied with the FTCA's requirement that the Plaintiffs must first present their claim in writing to the appropriate federal agency "and so their claim should be dismissed as to the United States for lack of subject matter jurisdiction." *Id.* (citing 28 U.S.C. § 2675(a)).

Plaintiffs do not dispute that the Attorney General's designee has certified the Federal Defendants or that they have not complied with the FTCA's procedural requirements. *Pls.' Opp'n* at 67-71. Instead, their singular point of opposition is that "the Federal Defendants violated a host of criminal and civil laws that disqualify them for a certification under the Westfall Act" and thus "this Court should reject the certification outright." *Id.* at 69-71. While Plaintiffs are correct that the Court may review the certification, the proper inquiry is not whether the Federal Defendants' conduct broke the law, but whether they were acting within the scope of their

employment. *See Davric*, 238 F.3d at 66 ("In order to strike the substitution of the United States, plaintiffs here must show that . . . [the defendant] was acting outside the scope of his employment at the time of the incident out of which the claims arose").

"Where a plaintiff asserts that a defendant acted outside the scope of his or her employment despite the Attorney General's certification to the contrary, the burden of proof is on the plaintiff" and "State law controls the determination of whether a federal employee was acting within the scope of employment." *Id.* (citations omitted). Under Puerto Rico law, courts:

> [M]ust consider the following three elements in deciding whether to impose liability under the doctrine of respondeat superior consistent with Puerto Rico law: an employee's a) [d]esire to serve, benefit, or further his employer's business or interest[;] b) [whether] the act is reasonably related to the scope of the employment[; and] c) [whether] the agent has not been prompted by purely personal motives. Among these elements, [t]he fundamental consideration for determination of an employer's liability is whether or not the employee's acts fall within the scope of his employment in the sense that they furthered a desire to serve and benefit the employer's interest, resulting in an economic benefit to the employer.

Vernet v. Serrano-Torres, 566 F.3d 254, 261 (1st Cir. 2009) (alterations in original) (citations and internal quotation marks omitted).

Plaintiffs allege that the Federal Defendants should not be certified because they lied on the search warrant applications, shared seized information with the DISH/NagraStar Defendants, allowed the DISH/NagraStar Defendants to accompany them during the search, and their entire criminal investigation was "nothing more than a ruse" to steal Plaintiffs' intellectual property. *Pls.' Opp'n* at 69-71 (quoting *Second Am. Compl.* ¶ 4). The Federal Defendants counter that "[t]he

allegations in this case involve actions the Federal Defendants took in furtherance of their investigative or prosecutorial duties on the United States' behalf" and that the "criminal investigation, including the execution of search warrants and the seizure of evidence at the plaintiffs' business properties . . . furthered the employer's business interest, which includes the investigation and prosecution of federal crimes." *Defs.' Reply* at 22 (citations and internal quotations omitted).

The Court agrees with the Federal Defendants. For Plaintiffs to establish conduct outside the scope of employment, they would need to offer well-pleaded facts alleging that the entire investigation was truly a ruse created for the purpose of stealing their intellectual property (or, at least primarily motivated by that improper purpose). Such allegations would establish that the Federal Defendants were not acting in their employer's interest of investigating possible criminal activity. As the Court has explained, however, Plaintiffs' allegations on this point—which offer little detail and no motive for the Federal Defendants to conspire with one private company against another—are too conclusory to support their claims.

Plaintiffs have not met their burden to show that, despite the Attorney General's certification, the Federal Defendants acted outside the scope of their employment. The Court will thus not reverse the substitution and the United States now stands in their shoes.

"Section 2675 [of the FTCA] requires that the potential plaintiff give notice to the government of the nature of the claim and the damages requested" and "[f]ailure to timely file an administrative claim with the appropriate federal agency results in

dismissal of the plaintiff's claim, since the filing of an administrative claim is a non-waivable jurisdictional requirement." *Santiago-Ramirez v. Sec'y of Dep't of Def.*, 984 F.2d 16, 18 (1st Cir. 1993) (citations omitted). Plaintiffs do not allege that they have provided notice, nor do they dispute the Federal Defendants' contention that—assuming the substation holds—this defect requires dismissal. For the reasons stated in *Santiago-Ramirez*, Plaintiffs' PTSA claim must be dismissed for lack of subject matter jurisdiction.

VI. CONCLUSION

The Court GRANTS the Federal Defendants' Motion to Dismiss (ECF No. 138). The Court DISMISSES Counts I-VII of Plaintiffs' Second Amended Complaint (ECF No. 130) as pleaded against the Federal Defendants.

SO ORDERED.

/s/ John A. Woodcock, Jr.
JOHN A. WOODCOCK, JR.
UNITED STATES DISTRICT JUDGE

Dated this 29th day of March, 2024